
# User's Guide

SC38-7107-3

**Note**
Before using this information and the product it supports, read the Notices and Trademarks information in Appendix E.

Seventh Edition (June 2006)

This edition applies to Hardware Management Console version H3.2 of Electronic Service Agent [tm] for pSeries. 

Edition Notice

# Contents

# About this user's guide

This guide provides overview information, setup, configuration instructions, and use information for Electronic Service Agent ™ for pSeries Hardware Management Console (p4 only), which may be referenced as Service Agent or SA for the remainder of this document.

## Terminology

You need to be familiar with the following terms in this manual:

### Hardware Management Console

The Hardware Management Console allows you to perform many hardware management tasks for the managed system, including configuring logical and affinity partitions.

### IBM Service Data Receiver (SDR)

The IBM data receiver, using the HTTPS POST mechanism with XML data for interaction between all SA platforms and IBM.

### Service Agent Connection Manager (SACM)

The SACM may utilize existing Internet connection or have a modem configured to communications through dialer structure. The Gateway Hardware Management Console and the standalone AIX or Linux SA may utilize the same SACM to communicate to IBM.

### Gateway Hardware Management Console

The Gateway Hardware Management Console is the system where SA central database is maintained for this complex, this is the default configuration. The gateway machine contains the central database and may contain the process for controlling the Internet or modem communications to IBM.

### Client Hardware Management Console

The client Hardware Management Console are the additional Hardware Management Consoles that use the Gateway to communicate to IBM. The clients do not have database capabilities, and must be configured as client Hardware Management Console to gateway.

### Service Focal Point (SFP)

Product application that resides on Hardware Management Console and AIX that delivers information to SA that needs to be reported to IBM. SA does no data collection in a Hardware Management Console environment, it only delivers the information that SFP directs it to handle.

### Enrolled machines

All HMC's supported machines will be enrolled using the CPU machine type, model and serial number. This information should be supplied by SFP to SA, you may have to fill the initial gateway data manually. (Do Not Use the PC type, model, s/n.).

### Standalone Electronic Service Agent ™ for pSeries and RS/6000

The AIX or Linux standalone Electronic Service Agent ™ for pSeries and RS/6000 may be installed on the operating system in the Hardware Management Console environment, but will not collect any data in a Hardware Management Console controlled complex that is collected by the Hardware Management Console. A common SACM may be used to connect all SA applications to IBM.

# Understanding Service Agent

This chapter presents general information about Electronic Service Agent ™ for pSeries (p4) Hardware Management Console.

## What is Service Agent?

Electronic Service Agent ™ for pSeries (SA) is an application program that operates on a pSeries Hardware Management Console and accepts information from the Service Focal Point (SFP). It reports serviceable events and associated data collected by SFP to IBM for service with no customer intervention. The SA Gateway Hardware Management Console maintains the database for all the SA data and events sent to IBM, including any SA data from other Client Hardware Management Consoles.

Since licenses are checked by the IBM SDR whenever a call is made to IBM, only machines on IBM Warranty or MA can use Service Agent to report errors. Other non service data would still be reported to the appropriate collection points within IBM.

## What does Service Agent do?

Here are some of the key things you can accomplish using Service Agent for Hardware Management Console:

- Automatic problem reporting with Extended Error Data (EED); service calls placed to IBM without intervention
- Automatic and manual collection and transmission of Vital Product Data (VPD), Snap, and Performance data (PM/AIX) to IBM
- Automatic customer notification of configured events
- Network environment support with existing Internet connection or modem dial support

## What models are supported?

This level of Service Agent supports **all Models** of **Hardware Management Console** (prior to Release 4) controlled **pSeries** machines**.**

## How does Service Agent work?

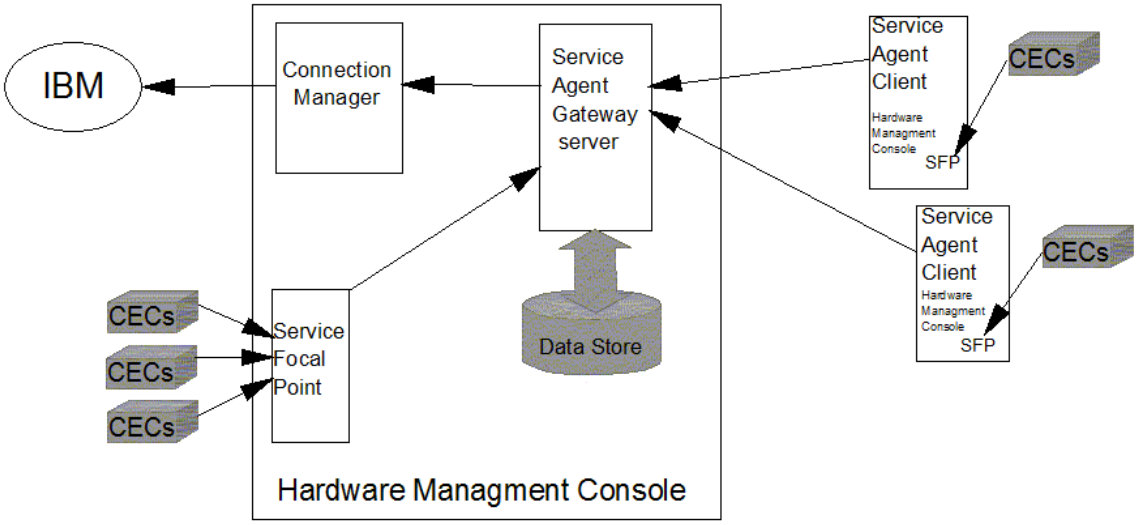
The Hardware Management Console machines have Service Agent installed as part of the Hardware Management Console Code. Updates to SA will be done with new releases of Hardware Management Console code. Once SA configuration information has been completed and the connection manager tested with Hardware Management Console enrollment, SA daemons wait for SFP to make a call request. Once SA receives a request, it is maintained in SA's database and the request is called into IBM. Results of the request are posted back into the database for information or later access with the SA user interface.

Once SA application is configured and started as a server or client host, the SFP will deliver to SA all the attached CEC information. Whenever an event occurs within a CEC, the diagnostics running on that CEC will notify SFP of the event. SFP will then decide if the event should be called into IBM and will pass the event to the SA running on the attached Hardware

Management Console. If it is a Client SA the event will be passed onto the SA Gateway server where it will be maintained, reported and tracked. SA will now process the event through the SA filters and if it qualifies will use SA Connection Manager communication link (internet or modem) to open a PMR with IBM. If the CEC is entitled to Service the PMR will be opened and the PMR number will be returned to the SA Gateway. If an email alert is setup for Open notification then SA will send the notification to the assigned email address.

The SA user interface may be invoked to monitor status of events and activities called into IBM.

**Block Diagram of SA on Hardware Managment Consoles**



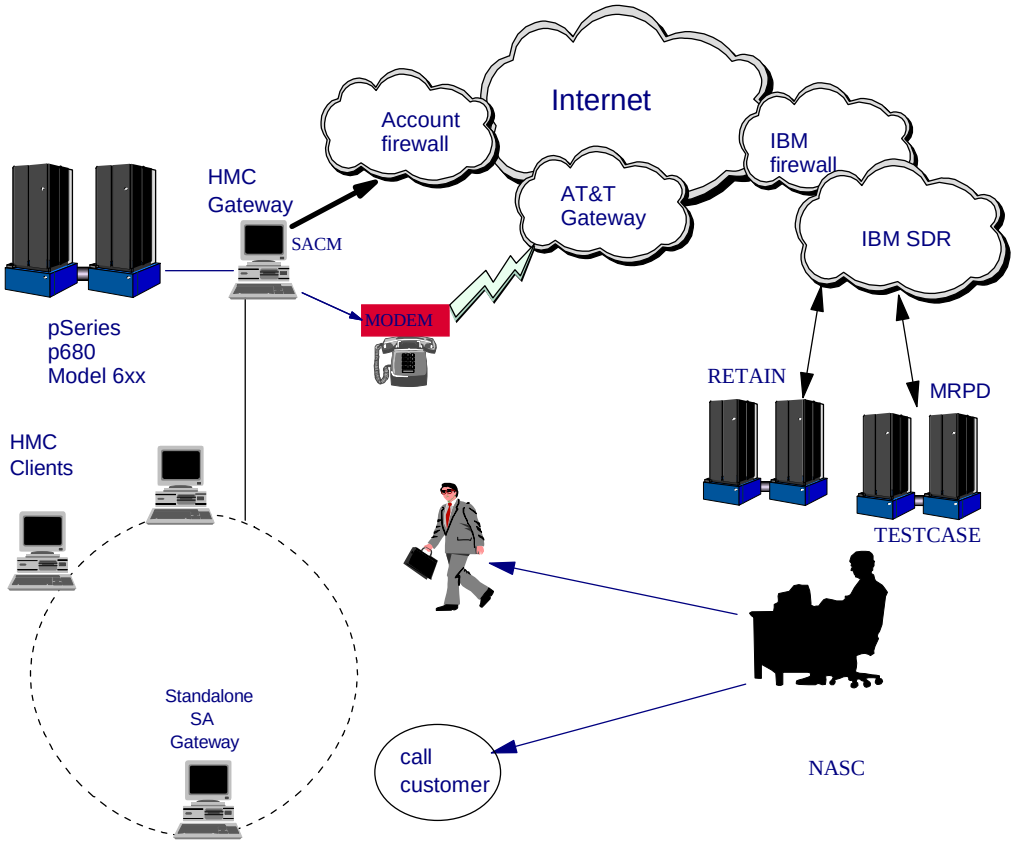

Manual functions executed from the SA user interface will be sent as a request to SFP to obtain the data from the selected CEC. SA has no direct connections to the CEC or LPARs running on the CEC. Test connections and test PMRs may be performed from the user interface. Maintenance of information that is contained within SA database can be scheduled or purged manually.

Hardware inventory (VPD) collection is done by the Hardware Management Console for each of the assigned CECs and is reported under the registered machine Type-Model_SerialNumber filename. For LPAR data collection is under the assigned LPAR hostname and contains only hardware assigned to that LPAR partition.

Performance Management data can also be collected from LPARs by Hardware Management Console if it is configured to do so. Both AIX or Linux PM data can now be collected by SA.

Simple Network Management Protocol support is now available for PMR and Internal SA error notification to local account monitoring applications. Service Agent generates the traps based on the ‘ibmServiceAgent.mib’ module. Locate this MIB module in the /usr/svcagent/lib directory or down load from ftp site and import it into your Management application.

The figure below illustrates a typical Service Agent monitored network.




**Understanding Internet, TCP/IP, and Modem**

The Service Agent Connection Manager (SACM) can communicate with IBM using Internet or the modem structure. The SACM can handle input from multiple configured SA gateway machines, Hardware Management Console or standalone AIX and Linux configurations. So a single Internet connection or modem is all that is needed to support a complex SA configuration. Redundancy can be achieved by using the secondary SACM as backup. So a primary Internet connection to IBM could be backed up with a secondary dial configuration assigned to a SA Hardware Management Console client host under the same SA network configuration. The two SACMs are controlled by a single CallController on the SA Gateway host. Make sure the secondary SACM has been started from the WSM Service Agent menu panel on the client host.

If existing TCP/IP structure allows connection to the Internet, then the modem may not be needed. The Gateway Hardware Management Console may have a modem attached to one of the serial ports. This will still allow the Dialer to utilize a local area call to connect to AT&T Gateway to access the IBM. Appendix C shows the proper basic modem setup for some IBM modems. The modem must be properly configured from the SA user interface, Dialer menu, prior to making calls.

Selection from the Hardware Management Console Service Applications for Service Agent allow for changes to the SA mode, gateway server or client. This requires you to have knowledge of the naming conventions and IP addressing used at the local complex. This same selection will facilitate Hardware Management Console hostname changes for SA. The Gateway Hardware

Management Console SA uses TCP/IP addressing to communicate with other Hardware Management Console Client machines if they exist. Using IP addressing, SA gateway receives information from the client Hardware Management Console systems and then forwards that information to the IBM.

## Understanding the SA Processes

There are four major components or processes that make up the Service Agent system:

- The Electronic Server System process running only on the Gateway Hardware Management Console
- The On Demand Server process
- The Service Agent Connection Manager process
- The User Interface

### Electronic Server System (ESS) process

The ESS process runs only on the Gateway Hardware Management Console and handles all requests for data input and retrieval from the centralized database.

### On Demand Server (ODS) process

The On Demand Server runs on all Hardware Management Consoles defined and handles all SA communication activities for that host. The ODS sends data to the ESS process as necessary, or makes a call to the IBM.

Events from the SFP are reported to IBM directly using an Internet connection or a modem that is attached to the Gateway server. The call times are fully configurable within the *Graphical User Interface.* SA also calls IBM to report that it is healthy, once in every health check interval.

### Service Agent Connection Manager (SACM) process

The Service Agent Connection Manager is a standalone process that can be configured to communicate with IBM using an existing Internet connection or modem. It may exist on any Hardware Management Console or standalone AIX or Linux machine and can support multiple SA Gateway connections. The account guideline would be to use the latest available SACM as a common connection. A primary and a secondary CM may be configured within the same SA Network configuration, they should be of course on different host on the Network.

### Graphical User Interface (GUI)

The Graphical User Interfaces allows the user to setup and define Hardware Management Consoles that SA monitors. The GUI is invoked from Web-based System Manager (WSM) by selecting Service Agent from the Service Applications. Then WSM Service menu, select TASKS for Service Agent User Interface. To initiate the Advanced SA User Interface select *Register and Customize Service Agent* from the available tasks.


It is used for advanced functions and customization of the system as well as configuration for complex systems and multilevel networks. A logon password is utilized which is defaulted to "password". It is recommended this password be changed after the initial install and stored in a safe place for security purposes. See Chapter 4, *"Learning about the SA Configuration interface*", for more information.

Additionally Service Agent can send e-mail notifications to contacts relating all or limited machine problem information. The e-mail notification functions must be configured before they become active. See Chapter 5, "Advanced Configuration Tasks", for information on how to configure e-mail notifications.

If the user interface hangs and can not be exited normally, the WSM interface has the ability to kill the GUI and allow for recovery. The WSM interface also controls the starting and stopping of the SA major processes and determines if the SA is going to be a client SA or a gateway (server) SA. If the Hardware Management Console hostname changes, then the *Change Service Agent Mode - (server/client)* is used to redefine the SA usage again.

# Prerequisites

This chapter presents prerequisite activities that need to be verified or completed prior to activating Service Agent on the Hardware Management Console.

__ 1. Review the following preplanning section.

__ 2. Ensure the Hardware Management Console & LPAR hostnames are resolvable either by local (/etc/host) or DNS, see note.

__ 3. Validate filesets installed such as rsct.core* and csm.client on Hardware Management Console & LPARs, check that any host changes have been correctly updated in rsct config files, see note.

__ 4. Ensure Inventory Scout Services is set up for each managed system and partition, see note.

__ 5. Ensure Service Focal Point has the Automatic call-home feature enabled, see note.

__ 6. If PM/AIX data is to be collected Hardware Management Console firmware must be higher than Hardware Management Console 3.2 and SA H2.1. Standalone AIX SA code is not required on LPAR. Reference Performance Management User's Guide SC30-3552-01, the latest documentation and code can be obtained from the following URL:
ftp://ftp.software.ibm.com/aix/service_agent_code/pmaix

__ 7. If e-mail notification is to be sent from the Hardware Management Console, ensure mail service is configured. If known mail server is network accessible from the Hardware Management Console, then that mail server may be used for SA mail notification.

__ 8. A p4 HMC SA gateway may now utilize a p5 HMC that is at GA6 or higher firmware and has its SACM properly configured.

**Note:** Reference Hardware Management Console for pSeries Installation and Operations Guide SA38-0590-7 Eighth Edition (November 2003) or later.

## Preplanning

Early planning may save you valuable time and prevent aggravation later. Understanding how to setup Service Agent application to best cover your IT complex should make the SA experience much more enjoyable. This section may answer some of the basic questions about SA and assist you in your decision making and placement of the SA components.

One should consider the following aspects:

__ 1. The only point in the Service Agent arena that can be shared by all 3 pSeries versions (Hardware Management Console, AIX, Linux) is at SA Connection Manager. The SA client of one OS cannot communicate with the SA Gateway of a different OS. Do not attempt to configure a standalone AIX SA client on a LPAR to the Hardware Management Console gateway controlling that LPAR.

__ 2. All communications between the SA Gateway and IBM is now encrypted and is secure using Java SSL no matter which communications method is selected. Using the dialer structure only makes AT&T the Internet Service Provider (ISP) and the modem connection is a much slower network.

__ 3. Is there an existing high speed Internet access available to communicate with IBM, configure to use it.

__ 4. SA supports multiple Connection Managers, one could use high speed network connection while the secondary could be configured for dialer backup.

__ 5. Which host would best support the Connection Manager:

- CM can be installed on a Hardware Management Console, standalone AIX or Linux host. It does not have to be a Hardware Management Console SA Gateway. If AIX or Linux CM is being used, that must be installed and activated from the associated SA package, get the latest level of that code from the SA URLs:
  ftp://ftp.software.ibm.com/aix/service_agent_code/AIX
  ftp://ftp.software.ibm.com/linux/service_agent_code/LINUX/
- CM can be controlled by a designated Master SA Gateway and that is protected by changeable password. This prevents different Gateways that are using SACM from changing the communications method set from the Master Gateway.
- Communications to and from CM host can pass though secure network firewalls.
- Hardware Management Console CM will always be started on port 1198 with secure mode against all available interfaces. Any other configuration must be manually changed from /usr/svcagent/bin/sacm script.
- Uses Java POST for secure https transfers, slower but secure. This communications method can pass secure firewalls, proxies, and use of NAT devices to obtain access to an available high speed Internet path.
- Hardware Management Console CM could support your AIX SA Gateways or Hardware Management Console SA may use the AIX CM.
- Always utilize the latest level of SA CM as the primary CM for the account.
- Primary and Secondary CM host can be used as backup, one Internet, one Dial. The two Connection Managers could be on the same Hardware Management Console SA Network configuration, one on gateway another on SA client Hardware Management Console host.

__ 6. The Hardware Management Console SA splash should be blue like the one on front page of this document. All Hardware Management Console SA applications with red splash should be upgraded to the latest Hardware Management Console firmware and blue splash SA by July 2005. The Independent Data Catcher (IDC) that supported the early Red splash has been sunset as of June 30, 2005

# Activating Service Agent

This chapter explains how to start up Electronic Service Agent ™ for pSeries, Hardware Management Console.

## Obtaining Service Agent

Service Agent for Hardware Management Console is part of the Hardware Management Console software and it comes either pre-installed, or as part of the recovery or upgrade CD.

## Starting Service Agent

Service Agent processes will be turned off on a new system or after recovery. On new installs the Hardware Management Console hostname is a default name and should have been assigned a new name to fit the customers network environment. Once the hostname is assigned and the determination as to the type of SA, Gateway or Client, has been made, use the Service Applications: Service Agent menu from WSM to activate SA (only valid TASKS selectable). You can follow the start status in secondary window, after validating start processes, please close window. To check what command was executed, click on Commands radio button instead of Messages. Status portion will now reflect the current status of SA on this Hardware Management Console.

Use the Service Agent panel for starting the processes when the account is ready to support SA. On the Hardware Management Console Gateway the modem and phone line should be connected if they are being used. Check the physical connections to determine this. If using the Internet make sure Hardware Management Console has connectivity to network. If Hardware Management Console is a client then start SA only after the network is setup properly. Do not start SA processes if the network is not configured on the Gateway or Client Hardware Management Console.

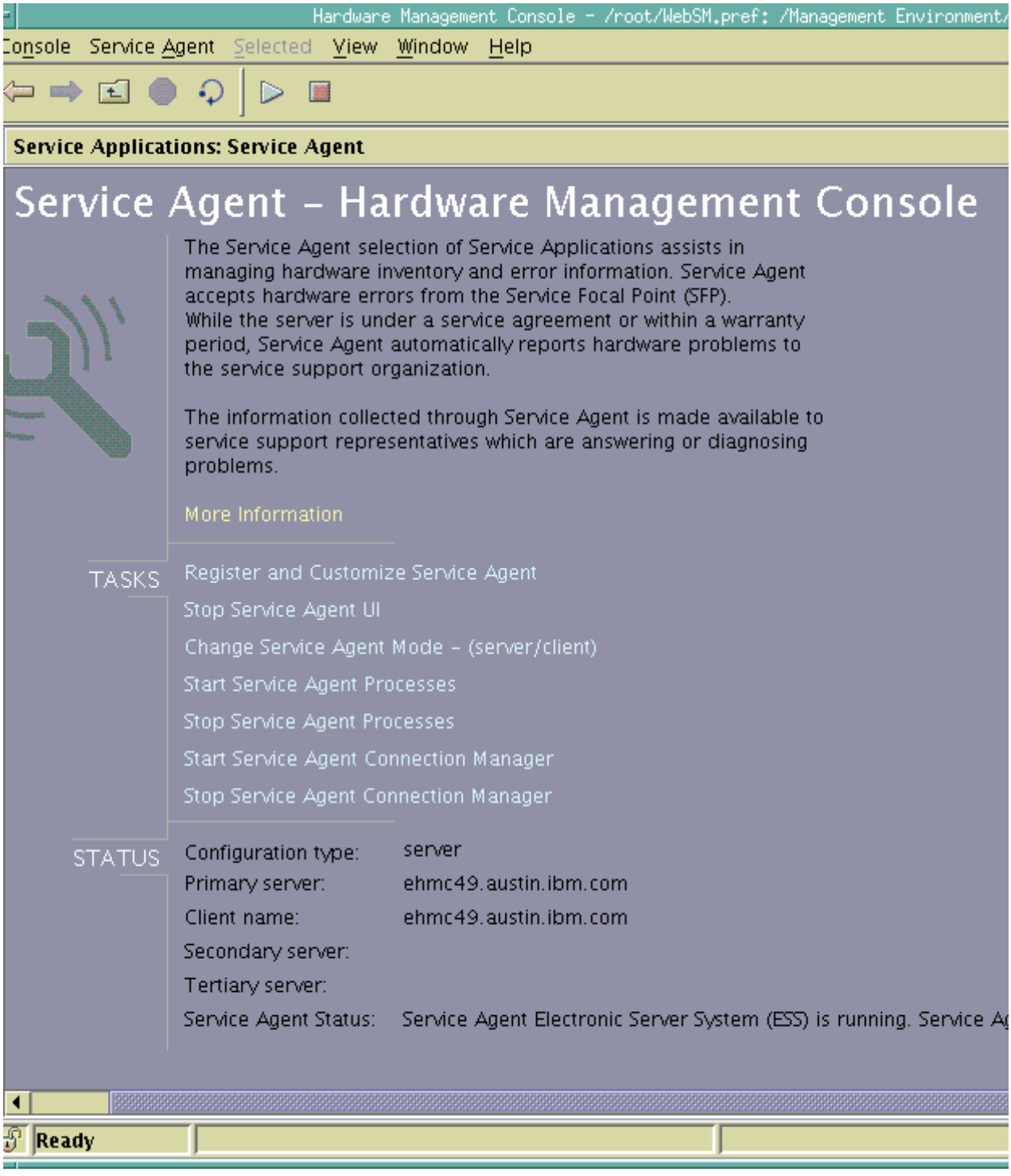
**Note:** Refer to prerequisites section if host network was changed manually.

Use the ‘Change Service Agent mode panel’ to set the SA Gateway or SA Client environment. Once selection is completed you can use the chapter "Configuration Task" to setup and configure the Hardware Management Console SA requirements.

On the change SA mode panel for a gateway server, both the Gateway and Client hostname should be the same. If settings are for client, then the client hostname will match this Hardware Management Console hostname, and the Gateway hostname will have to be updated to reflect the Hardware Management Console SA gateway host. The Hardware Management Console client has only the ODS process running and that forwards data to and from the SFP running on the client Hardware Management Console to the database process on the gateway SA Hardware Management Console.

Anytime that the Hardware Management Console hostname is changed, the SA application should be stopped and the "Change Service Agent mode" should be used to correct the hostname setting for SA. After this mode change, the SA application can be started again. If this is a client Hardware Management Console then the SA Gateway database needs to be changed to reflect the new client hostname, before starting the SA client.

## WebSM Service Agent main menu



## Stopping and Starting the Service Agent processes

There may be times you want to stop or restart the SA daemon processes.

### Stopping the Service Agent daemons on the Hardware Management Console

Follow the steps below to stop the Service Agent daemon on the Gateway server:

- Bring up the Service Agent Panel from the Hardware Management Console WSM User Interface
- Click Stop Service Agent processes

You have now ended the normal Service Agent daemon processes, and removed the inittab entries. If the SACM is running on this Gateway server it will not be stopped unless you wish it to be and you must also select Stop SACM from the Service Agent Panel. Remember the SACM might be supporting other SA gateways.

### Stopping the Service Agent Connection Manager on the Hardware Management Console

If the SACM is running on the Gateway server and it needs to be stopped for some reason you must also select Stop SACM from the Service Agent Panel of the WSM User Interface.

### Starting the Service Agent daemons on the Hardware Management Console

After you have stopped the Service Agent daemons, you will have to restart them on both the Gateway server and the client machines. Follow the steps below to restart the Service Agent daemons on the Hardware Management Console machines:

- Bring up the Service Agent Panel from the Hardware Management Console WSM User Interface.
- Click on the Start Service Agent processes option
- Be ready to press any key to go into logging mode to check or change the status of logging.

You have now created new inittab entries for the ESS & ODS daemons processes which will restart the Gateway Hardware Management Console SA processes. Only the ODS daemon is started on a client Hardware Management Console. If there is a SACM process it to will be automatically started. If keystroke is done in working window the logging and debug options for the SA processes will be given.

### Starting the Service Agent Connection Manager on the Hardware Management Console

If the SACM is stopped on the server and it needs to be started it can be selected with the Start SACM pushbutton from the WSM User Interface Service Agent Panel. This only starts the SACM process and has no effect on SA Gateway or client processes. On start of SACM you also have the option to enter Debug mode for SACM, monitor the detail working window for key board prompt. Current Debug status will be shown and the valid options will be given, select the necessary option number.

# Learning about the Service Agent User Interface

The Service Agent User Interface (SAUI) is used for various functions. For example, setting local user notification entries and customization of the system as well as configuration for complex systems.

This chapter will help you learn how to use and navigate the user interface.

- How to access the User Interface
- Use of passwords
- Understanding the left side or Navigation pane
- Category Selectors
- Add and Delete functions
- What is active when category is selected

## Accessing the Service Agent User interface

The GUI is invoked from Web-based System Manager (WSM) by selecting Service Agent from the Service Applications. The Service Agent WSM is broken into two main sections TASK and STATUS. The lower or STATUS section keeps you informed as to how this Hardware Management Console is configured (server/client) and the status of the SA processes. Under the TASK section in the middle, you can control and access SA. This is how you start and stop the processes, change the function or hostname update, and access the user interface.

From the WSM menu select TASKS "*Register and Customize Service Agent*" for User Interface.

**Logging on**

The SA User Interface requires a password to gain access to the application . The initial default password is **password**.

The administrator should change this password to one that is unknown to anyone but himself and or authorized personnel to protect the Service Agent configuration setup from unauthorized modifications. Typing a wrong password causes an error message to be displayed indicating the password entered does not match the one expected. If the error message comes up, click **OK** and retype your entry to try again. You have up to six chances to type the password correctly. On the sixth mismatch, the logon quits and the User Interface must be selected from WSM again. While Service Agent is waiting for input and matching the password, a *Prompting for Password* progress window is displayed. After a successful password match, the user interface is displayed.

If password has been changed and new password forgotten the Hardware Management Console recovery disk has to be restored doing a clean install. This will restore the default password setting.

## Understanding the Configuration screen

The user interface is divided vertically into two panes – a navigation pane on the left and a detail viewing pane on the right.

The buttons at the top of the navigation pane are called *category selectors*. Each category determines the type of information that is displayed in the detail window to the right. The very top buttons (located in the Menu bar) are the *File* and *Help* dropdown buttons. From the *Menu* bar, selecting the *File* dropdown enables an *Exit* option. Also in the Menu bar is the *Help* dropdown. Clicking the *Help* dropdown displays the *Show Help* and the *About* options.

At the very bottom of the navigation pane are two buttons labeled Add and Delete. These buttons are highlighted when enabled. If they are not highlighted when you think they should be then check the *category selectors* you may have the wrong category selected.

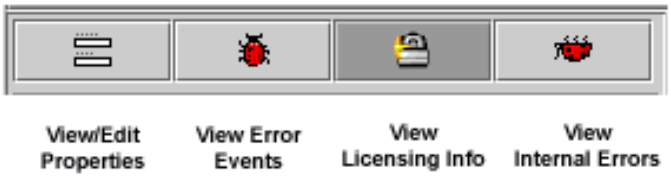
To edit the detail information to the right, click in a field and make the necessary changes. Mandatory fields are indicated by an exclamation mark; Fields which cannot be changed are flagged with a padlock. Click the **OK** button at the bottom of the detail pane to save your changes, or click **Cancel** to abandon your changes. If you fail to click **OK** before switching to a different screen your changes are not saved. This is equivalent to clicking **Cancel**. After clicking **OK**, if you have missed any mandatory fields or if you have entered data which is incorrect for the field, a window pops up listing the problematic fields. Mandatory fields are marked with an exclamation ( **!**), invalid data is marked with an **X**. Additionally, the field name in the property sheet turns red. Also, if you are selecting an item from a list, you can type the first letter of the desired item to move quickly through the list.

### Category Selectors

There are four category selectors available which determine the type of information displayed in the detail window when a category button is selected. They are:

- View / Edit Properties
- View Error Events
- View Licensing Info
- View Internal Errors

In many cases the right hand detail screen may be blank. This is because the selected category may not have any information available.



**View/Edit Properties button**

The View / Edit Properties button is identified by the icon that looks like an equals (=) mark. While the category is selected, all *Properties* buttons of the navigation pane on the left side are active and available. This is the selector that is used most of the time and must be the one active when ever any configuration data is changed.

**View Error Events button**

The View Error Events button is identified by the icon that looks like a red bug. Selecting this category along with the Network properties button displays a table of all of the errors Service Agent has recorded within its defined network. Error Event or PMRs associated with individual machines can be displayed by selecting this button and an individual machine.

**Note**: The table may be reorganized by dragging column titles to where you wish them to be displayed. Sorting is automatic from the first column, dragging the column to the left most table position sorts the table on the selected title.

The following list describes the content of the Service Agent Errors Events summary, the Internal Errors are also listed in this category:

**Host** The name of the machine for which information is being displayed.

**Timestamp** The year, month, day, and time the Error Event occurred.

**Icons** Icon quick indicators to status.

**Status** Status indicates the current state of a selected error. Possible states are:

**Pending** Indicates an entry that is set to be sent to IBM. It is the initial status state which triggers the Service Agent CallController to connect to the IBM SDR. If the status is some other state, setting it to pending again causes the entry to be resent.

**held** Indicates that the Error Event determined to be reportable was held rather than reported to IBM.

**open** Indicates that the Error Event was sent to IBM and a Problem Management Report (PMR) was generated.

**duplicate** Indicates an attempt was made to open a PMR that was already opened. If the same Type, Serial number, Description, and error number is opened before a previous PMR with the same error is closed a duplicate status is returned.

**failed** Indicates that the Error Event failed in the attempt to open a Problem Management Report.

**closed** Indicates that the Event previously opened with IBM has been closed.

**PMR# / PMR Number**
PMR stands for Problem Management Report. The number in this field is the PMR number returned from IBM when an Event or problem was opened.

**Error# / Error Number**
This could be the 8 digit unique id from the error log entry that was captured, or the Service Reference Number (SRN) generated by the diagnostic analysis of error.

**Description** Description of the error that was generated.

**Resource** The logical resource name of the component that failed.

**Type** The System type of the node on which the error occurred. (e.g. 7040 )

**Class** Describes whether the error occurred in hardware or software, is an operator message, or is undetermined. Following are the definitions for the class descriptors:

**H** Indicates the error is a hardware failure.
**O** Indicates the error is an operator message.
**S** Indicates the error is a software failure.
**U** Indicates the error is undetermined.
**SURVLANC** Surveillance error. Normally this is not reported to IBM
**OS** Meaning the error has occurred on the operating system.

**Dups** Counter of duplicated error events that occurred since the original entry was generated.

**Last** Last time the Error Event occurred.

**When Status Checked** Last time the opened status of an error event was checked for closure.

**Detail Error Event Pane**
The lower right panel displays details of selected event in a scrollable pane and contains all of the previous listed summary fields plus the following detail entries.

**Error Details** Contains specific details for the error that occurred.

**Status Details** Contains results of transmission attempts to IBM for a specific error event or PMR entry.

**View Service Agent Internal Errors button**

The View Service Agent Internal Errors button is identified by the icon that looks like a red bug that is on its back (feet up). Selecting this category along with the Network properties button displays a table of all of the internal errors and exceptions Service Agent has detected while running functions. Both internal program exceptions and external access failures for host creation or program running are displayed.

The following list describes the content of the Service Agent Internal Errors category:

**Host** The name of the machine for which information is being displayed.

**Timestamp** The year, month, day, and time the error occurred.

**Error# / Error Number** The number the system affiliates with the type of error generated.

**Error Details** Contains specific details of error that occurred.

**Status Details** Contains results of transmission details to IBM for a specific event or PMR entry.

**When Status Checked**
Last time the opened status of a specific error event or PMR was checked for closure.

**Details** Display any appropriate error information about the internal error if available.

**ID** Internal identification number. Typically " -1".

**Description** Description of the error that was generated.

**Resource** The logical resource name of the program component that failed. Typically this will be "exec".

**Class / Error Class** Typically this field indicates "none".

**Detail Error Event Pane** The lower right panel displays details of selected event in a scrollable pane.

**View Licensing Information button**

The View Licensing Information button is identified by the icon that looks like a padlock. Selecting this category, along with the Network properties button, displays a table of license status information for all machines defined. Specific tables associated with individual machines can be displayed by selecting this button and an individual machine.

The following list describes the content of the licensing information category:

**HeartBeat**

The HeartBeat status indicates whether a monitored machine has reported to the Gateway within the defined time limit. A good HeartBeat is indicated by a Green Flag reflecting that the machine has good communication with Gateway. This also applies to the Gateway itself, the ODS processes on the Gateway also communicates to the ESS.

A missing HeartBeat is indicated by a Red X. The Red X indicates the client Hardware Management Console is not communicating with the Gateway within the specified time limit. Some reasons for missing the HeartBeat include, different version levels between the Gateway and the monitored machine, the Client code (ODS) not running or needing to be restarted, possible slow network delays causing the client to miss it's HeartBeat window, or the client Hardware Management Console is down.

To adjust the HeartBeat window, go into the Linux Hardware Service template on the individual machine and change the HeartBeat and/or the HeartBeat Delay accordingly. To be notified when a Hardware Management Console misses a HeartBeat, you can set the heartbeat flag in the Email Notification template.

**LockStatus**

The LockStatus status indicates whether a system has been locked out and all errors detected are ignored or whether it is unlocked and the machine is being monitored.

A Green Flag indicates the system is unlocked and is being monitored. A Red X indicates the machine is locked out and is being ignored.

To lockout a machine go the *Administration* folder and access the *Lockout Machines* function. Select the machine you wish to lock out and click the **lock** button. This in turn changes the LockStatus to a Red X.

After completing the task on the locked out system, you MUST unlock the machine by accessing the *Lockout Machines* function again, select the locked machine, and click the **unlock** button.

**Status**

The Status field indicates the Linux Hardware Service Template status of the machine. Refer to the section on the Linux Hardware Service Template for detail explanation of the Status.

**Expiry** This is the date the enable license expires.

**Node** The name of the machine for which information is being displayed.

**Vendor** The name of the company that manufactured the selected machine or device.

**Module** This field indicates the name of the Module or Template that is licensed. An example of this is the Linux Hardware Service template.

**Comment**

This is a general comment field containing additional information pertaining to the licensed template.

**Environment Template Pane**

The lower right panel displays details of selected item in a scrollable pane.

## Add and Delete Buttons

The Add and Delete buttons (located at the bottom of the navigation pane) are enabled and disabled depending upon which property button is selected. In addition, different options are displayed under these buttons depending upon the actual functions available to the selected property.

**Property Selections**

Properties are located in the Navigation Pane below Category Selectors and above the Add and Delete buttons**.** Click any Property selection to see corresponding information in the detail pane on the right or additional function selections. If a property selection has a key pointing to the right, it means there may be another level of detail below it. Click the key to expand the view. A key pointing down indicates that all lower levels are displayed. To hide that level, click the key again. You can use this hierarchy to view information at different levels; for example, you can view data for the entire network or department, or just for an individual machine.

**Table Sorting Order**

When information is presented in a table, as in an error list, you can change the sort order by dragging a column title left or right as needed. The table is sorted based on the contents of the first column using the columns to the right to break ties. Click a row to display details of the entry.

**Network Property**

The property selection labeled Network is considered the main infrastructure property of the Service Agent system. This property displays the hierarchy tree used to view and configure information for individual machines and groups. When the Network property in the Navigation pane is highlighted, the Add button at the bottom is enabled.

# Configuration tasks

This chapter contains many How To....s of various tasks that you can perform from within the Configuration interface. The tasks are grouped into the following categories:

- How to do basic configuration
- How to add or create additional configuration entries
- How to remove, delete or test certain configuration entries
- How to perform other Service Agent functions

## How to Initially configure SA

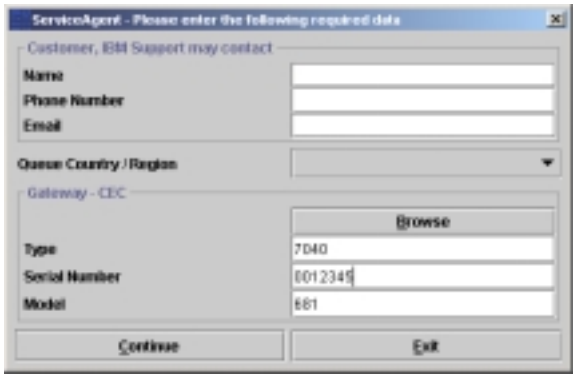
### Hardware Management Console SA Password

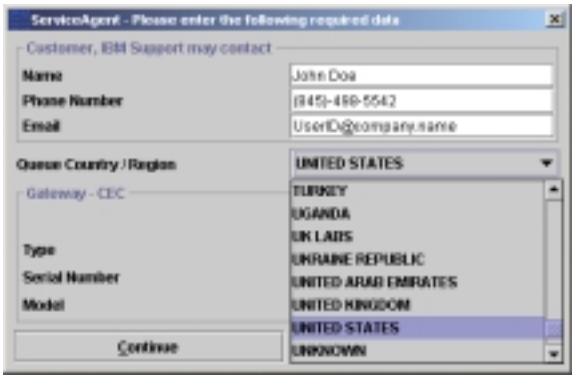
Whenever SA User Interface is started you will see the Hardware Management Console SA splash, then you should see the password prompt window. If you see the splash but get no password prompt the SA code is not active on the Hardware Management Console or no communications to the ESS process pointed by the properties file.


Please enter the password "password", this may be changed later for security.

### Initial Hardware Management Console SA menu

The first time the SA is invoked on a new install or after a clean restore you will be prompted for the basic information about account and machine information for this Hardware Management Console. The information for the CEC may auto fill, if not please fill in using the primary CEC information and not the PC information.




Please fill in the customer information and select the correct country from the pull down window. Then hit the Continue pushbutton to complete the prompt.

### Hardware Management Console SA Network menu

With the initial Network information completed, the SA user interface will initialize with the Network template being displayed. Additional information may be added to template at this time.

__ 1. Complete as many of the fields as possible, to better define account information. The "Telephone Number" will be used for primary contact if entered, instead of the "Contact Phone Number". The "Comments" will be added to all PMR data records.
__ 2. Click **OK**.

Once the Network information has been saved, you must decide which path of communications you will be using to communicate with IBM.

__ 1. If this Hardware Management Console SA configuration will be a client Hardware Management Console, go to *Make a Client Hardware Management Console*.

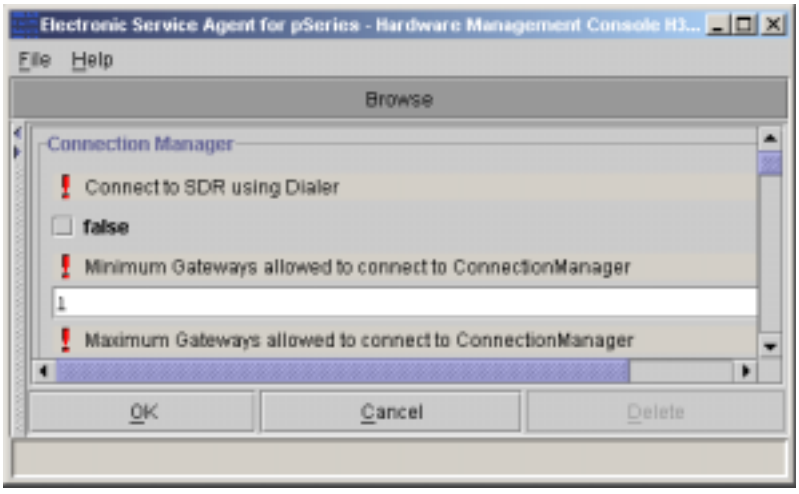
__ 2. If you are using the modem dial structure then the default Connection Manager is good and you only have to configure the Dialer template, see *Configure Dialer menu*.

__ 3. If you are planning on using an existing Internet, then your dialer does not need configuring but you must configure the SACM to **not** use the dialer at *SACM menu*.

__ 4. If you are planning on using an existing Master SACM, then you need to change the default Call Controller configuration. Go to *Configure Call Controller* menu.

### Configure Hardware Management Console SACM menu

Expand the Network by clicking on the key icon to the left on Network icon, then expand the Hardware Management Console Gateway machine, now select Connection Manager. Your doing this step because you are not planning on using the dialer. The normal item that you need to configure on Connection Manager is to set the "Connect to SDR using Dialer" to false.

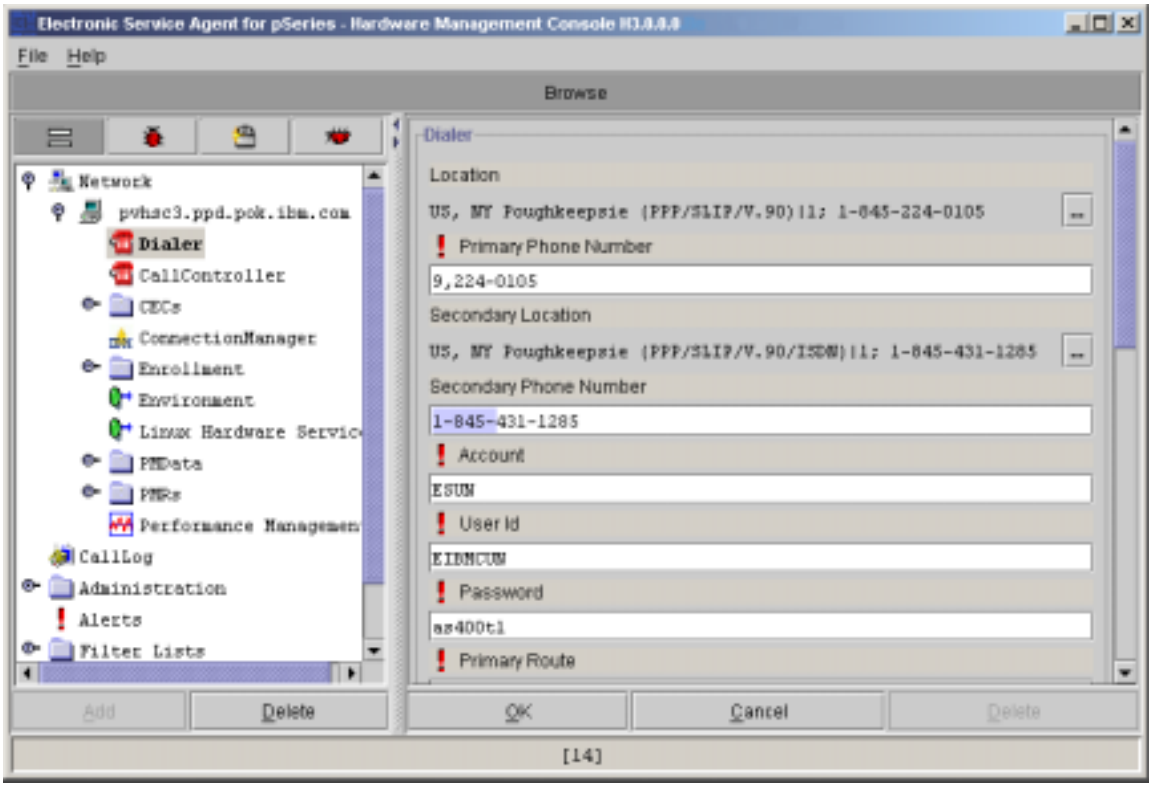



The other fields should be setup correctly with the defaults. If you are required to use a Proxy Server to gain access through a firewall to the Internet, then you will need to add that information to the correct Proxy Server items at the bottom of the template. After clicking OK to save the template you should check the CallLog to make sure the SACM Update was successful. If it

posts a fail, then there is a problem communicating to SACM. Check that SACM is running and the CallController template points to the correct *hostname:port* for CM being used.

**Configure Dialer menu**

Expand the Network by clicking on the key icon to the left on Network icon, then expand the Hardware Management Console Gateway machine, now select the Dialer.




**You are now in the Dialer property.**

__ 1. From the Location field, above the primary phone number, select the phone list browse box. This will post the Phone List with the country and city the modem calls to.

__ 2. By opening the Location field, selecting the proper country, then click Details, select city and local phone number, additional fields within the Dialer property are filled in.

__ 3. Check the *Primary Phone Number* field to make sure it is filled in and correct. If it is not filled in or is incorrect, fill it in or make the number correct.

__ 4. Depending on the local phone exchange, this number may need to be modified to utilize your outgoing number and area code requirements.

__ 5. Check the *Secondary Phone Number* field to make sure it is filled in and correct. If it is not filled in or is incorrect, fill it in or make the number correct.

__ 6. The *Account, User ID, Password, Primary & Secondary Routes and DNS* fields are automatically filled in and should not require changing or alterations.

__ 7. The default TTY# is set to ttyS1 which relates to Com2 port. Change to correct TTY serial port number if required.

__ 8. If the default modem does not match your attached modem, click the **Modem drop down** box. Select the Modem that matches the one installed to your Gateway server. See Appendix C, *Modem Setup*, for modem initialization and setup if you need more information.
**Note**: Opening and selecting a modem produces the values used in the Reset String and Init String fields. These modem strings are on an AS IS basis. They may need to be modified depending on the environment setup of your system.

__ 9. If you have a rotary or pulse phone system, dick the **Dial Type dropdown.** Select the *dial type (pulse)* to match the type of phone line.

__ 10. Click the **Baud Rate dropdown.** Select the highest *baud rate* that your modem uses.
**Note**: Selecting a baud rate greater than what the modem supports could cause the dial out process to fail. The flag entry *Verify Baud Rate Before Dialing* is defaulted True.

__ 11. If necessary, modify the default *reset and init strings* to work with the modem.

__ 12. Click **OK** to save your Dialer property configuration data.

__ 13. Check the CallLog to make sure the SACM Update was successful. If it posts a fail, then there is a problem communicating to SACM. Check that SACM is running and the CallController template points to the correct *hostname:port* for CM being used.

__ 14. Go to *How to Enroll*.

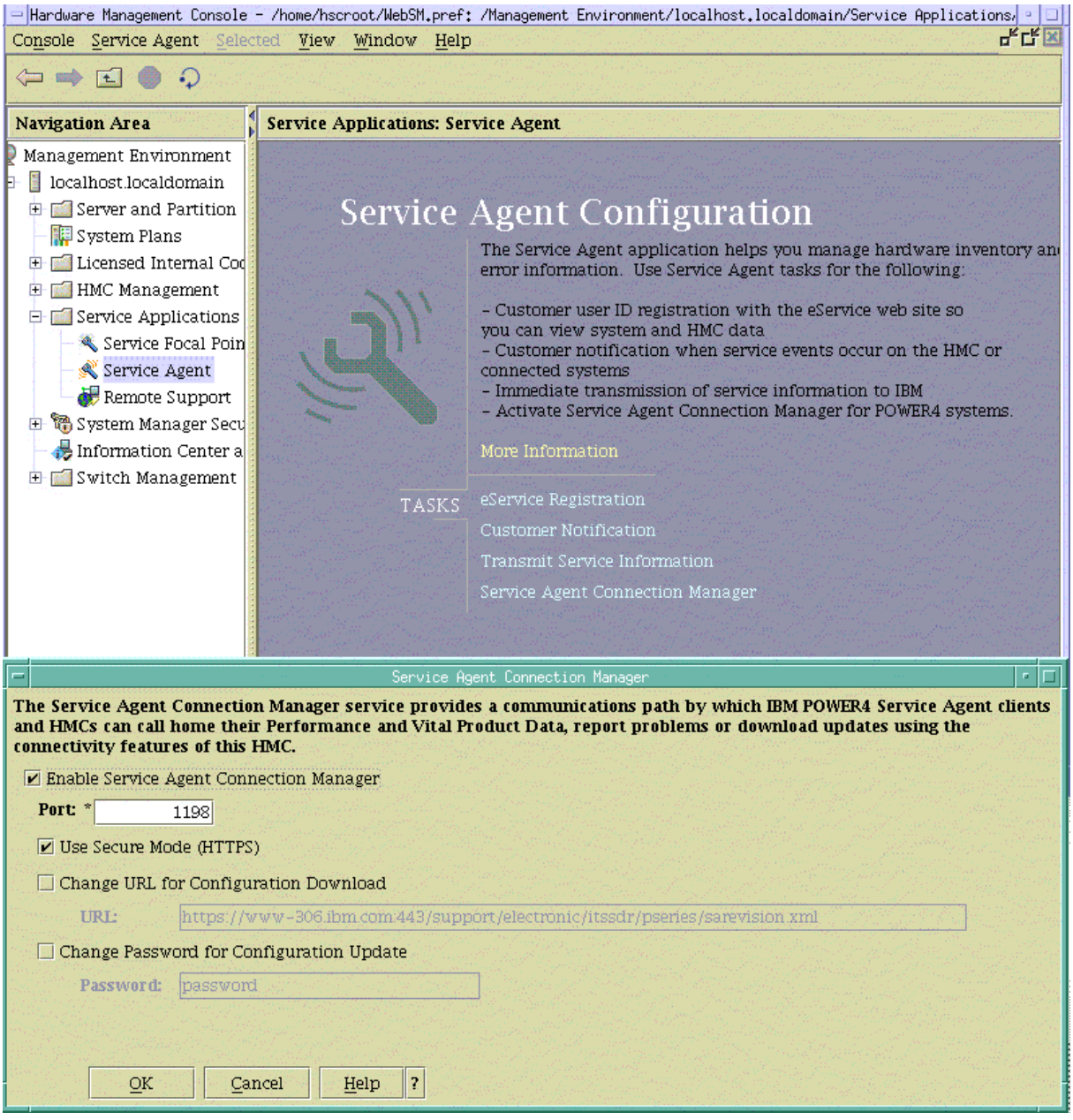
**Configure Call Controller**

By selecting the CallController under the Hardware Management Console gateway machine that you wish to change the default configuration of, all the detail fields become available to be modified. The default CallController expects to connect to the local SACM by the loopback communication interface.
So the **Primary URL to ConnectionManager** is set to *localhost:1198*, which is the loopback interface name and 1198 socket running secure mode.

Network connectivity must exist to the Master SACM host, and that fully qualified hostname may be placed in the **Primary URL to Connection Manager** entry with socket 1198 appended. A backup or secondary SACM may also be configured to CallController by adding the backup hostname and socket to the **Secondary URL to Connection Manager** field. If the primary SACM can not be reached the call will be attempted to the backup Connection Manager. Two Connection Managers may be configured now under one Network if available SA client host are configured in that network. The secondary CM could be activated on the Client host.

If the local Connection Manager is no longer needed on this Hardware Management Console, both the Connection Manager and the Dialer templates may be deleted.

If the Master SACM is isolated by a firewall then Proxy server may be required to access it. Check with the account network administrator and apply any needed Proxy information. If fields are not needed, please leave them blank.
The CallController may be configured to utilize a Master SACM on another Hardware Management Console (including p5 ), AIX or Linux OS host. This is done by setting the




**Primary or Secondary URL to Connection Manager** to *https://ForeignHostName:Port#*. If the Foreign host is a p5 HMC that is capable of running SACM check to see how it is configured by using WebSM process as shown in following object.
If the Secure Mode is not checked then the **URL to Connection Manager** should be entered as *http://ForeignHostName:Port#.*
Continue with to *How to Enroll*.

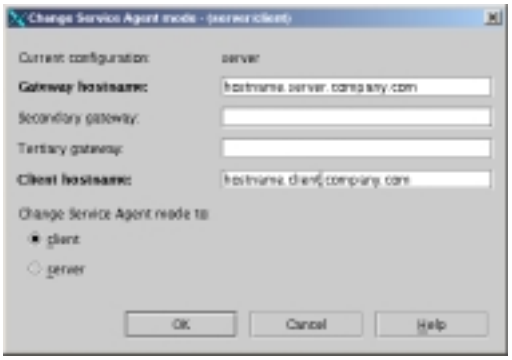
## How to Enroll

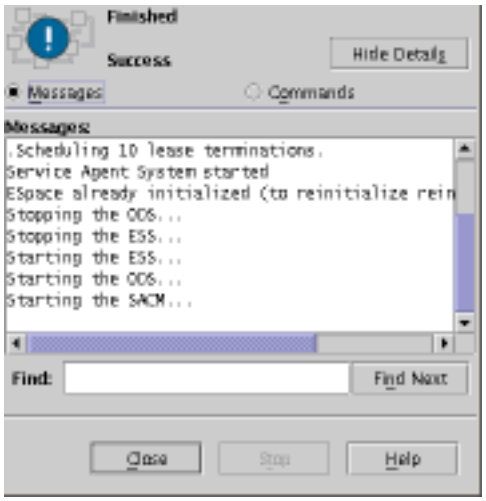
The Enrollment process with the SDR will return an SDR Enrollment ID and password for the particular machine requested. The Gateway will need to manage the enrollment of machines with the SDR and their associate SDR Enrollment ID/Password.

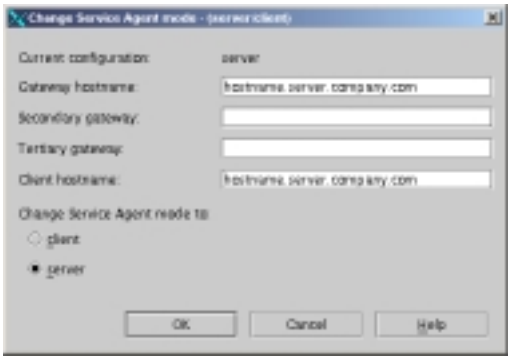
__ 1. Select **Administration** property.
__ 2. Select **Enroll**.
__ 3. Select the Hardware Management Console that you wish to Enroll, all machines supported by that Hardware Management Console will be enrolled.
__ 4. Click **Enroll**.
__ 5. Select Immediate, then select CallLog to monitor progress of communications.

**How to Make a Client Hardware Management Console**

__ 1. Select **Service Agent** menu on WSM Service Applications.
__ 2. Under TASK select **Change Service Agent mode**.
__ 3. On pop-up Change Service Agent mode window.
__ 4. Click **client** radio-button under **Change Service Agent mode to**.
__ 5. Change **Gateway hostname:** field to the hostname of the Gateway Hardware Management Console.




__ 6. Click **OK** to start the change.
__ 7. Close the message window when action is completed.

If it is a server both hostnames are the same.

If it is a client the hostnames will be different and point to the correct Hardware Management Console hosts client and gateway.

Don't forget to add this new client to Hardware Management Console Gateway configuration.

**How to Make a Server Hardware Management Console**

__ 1. Select **Service Agent** menu on WSM Service Applications.
__ 2. Under TASK select **Change Service Agent mode**.
__ 3. On pop-up Change Service Agent mode window.
__ 4. Click **server** radio-button under **Change Service Agent mode to**.
__ 5. Change **Gateway hostname:** field to the hostname of this Hardware Management Console (both client & gateway have the same hostname).
__ 6. Click **OK** to start the change.

**How to Update a Hardware Management Console Hostname Change**

__ 1. Select **Service Agent** menu on WSM Service Applications.
__ 2. Under TASK select **Change Service Agent mode**.
__ 3. On pop-up Change Service Agent mode window.
__ 4. Verify **server** or client radio-button under Change Service Agent mode is correct.
__ 5. Verify the new hostname appears in the correct **hostname:** fields. If new hostname does not appear in correct field, then manually enter the hostname. (On client host only the client hostname: will be changed.)
__ 6. Click **OK** to start the change.

## How to add or create additional configuration entries

**How to add a client Hardware Management Console**

__ 1. Select **Network** property.
__ 2. Click **Add**.
__ 3. Click **Child sub-menu**.
__ 4. Click **Machine entry** of the *Child sub-menu*.
__ 5. Complete all the required fields for the selected machine.
__ 6. Click **OK** to save the data.

**How to create a department of monitored Hardware Management Consoles**

__ 1. Click **Network**.
__ 2. Click **Add**.
__ 3. Click **Child**.
__ 4. Click **Department**.
__ 5. Type the **name** you want to use to describe this department or group.
(This example uses DEPT1 as the department name.)
__ 6. Click **OK**.
__ 7. Click **DEPT1** (or the name you used to create the department).
__ 8. Click **Add**.
__ 9. Click **Child**.
__ 10. Click **Machine**.
__ 11. Fill out the *Node Info* template and click **OK**.
This new monitored machine (designated by the name you give it) appears indented under the DEPT1 department name.

**How to add other standalone AIX or Linux SA client**

This **cannot** be done. Only Hardware Management Console clients maybe added to Hardware Management Console gateway configurations. The SA gateway / client configurations can only be done on like operating systems.

**How to specify the physical location of a machine**

Specifying the physical location of a machine helps service representatives provide prompt, quick service to monitored machines.

__ 1. Click the **Network** property folder.
__ 2. Click **Add**.
__ 3. Click **Form**.
__ 4. Click **Location**.
__ 5. Type the correct data into the *Location* template.
__ 6. Click **OK**.
__ 7. Scroll the details pane to verify that the *Location* template was completed.

**How to Add a Secondary CM**

Additional Connection Manager may be added to a Client host on the same network as the gateway. The CallController must be setup to direct backup communication and CM configuration to the secondary CM.

__ 1. Click on a specific monitored machine.
__ 2. Click **Add**.
__ 3. Click **Child**.
__ 4. Click Connection Manager
__ 5. Select if this CM will be using Dialer or connect by the Internet. If using Dialer you must add the dialer to this connection manager see following how to.
__ 6. All of the remaining fields may be taken as defaults, unless proxy information needs to be added for Internet access.
__ 7. Click OK

**How to Add a Dialer to CM**

Secondary CM would be added without a default dialer or dialer may have been removed from CM. The only add option here will be the dialer and the new dialer template will be posted for you to select the local dial number and ports to be used.

__ 1. Click on a specific monitored machine which host the CM.
__ 2. Click on the **Connection Manager**.
__ 3. Click **Add**.
__ 4. Fill in the Dialer template with primary and secondary phone numbers.
__ 5. Select the correct TTY port and the proper modem is necessary.
__ 6. When all templates fields are correct.
__ 7. Click OK

**How to define resource filters**

Resource filters allow you to specify certain devices so that they are not reported to IBM. This is particularly needed if the device is a non-IBM device not covered under warranty or a maintenance agreement (MA). You can define resource filters for the network or for specific monitored machines. This example uses a specific monitored machine.

__ 1. Click on a specific monitored machine.
__ 2. Click **Add**.
__ 3. Click **Form**.
__ 4. Click **Resource Filter**
__ 5. Type the *name of the resource* to filter or a *range of resources*.
__ 6. Click **OK**.
__ 7. Verify your *Resource Filter(s)* by locating the Resource Filter template in the details pane.

**How to specify thresholds**

Thresholds provide you with a way to prevent certain errors (for a network view or a monitored machine view) from being reported (by Service Agent) to the IBM Service data receiver.

Go to *Thresholds* in Appendix A to see how to find out how to determine errors (their id or number) that you can then use in defining thresholds.

__ 1. Select either the *Network folder* or a *monitored machine*.
__ 2. Click **Add**.
__ 3. Click **Form**.
__ 4. Click **Threshold**.
__ 5. Type the correct data into the *Threshold template*.
__ 6. Click **OK**.
__ 7. You can verify the Threshold entry. Scroll the details pane to the *Filter Lists folder*.
__ 8. Click **Thresholds**
__ 9. Scroll until you locate the error that you just added .

**How to lockout Service Agent on a machine**

The Lockout Machines template allows turning off or locking out SA on an individual machine. **CAUTION:** The locked out system will not report any errors until the lock is removed. Be sure to unlock the system after all maintenance work is performed.

__ 1. Under the Administration folder, click **Lockout Machines**.
__ 2. From the detail pane, select the monitored machine or machines on which you want to lockout Service Agent.
__ 3. Click **lock**.
__ 4. To verify the lockout, click the **Network** folder, then click the **Pad Lock** icon to display status. The machine's status should show a red X, indicating it is locked.

**How to add a SNMP Notification**

__ 1. Select a monitored machine for which you want to create a SNMP notification.
__ 2. Click Add.
__ 3. Click Child.
__ 4. Click SNMPTrap.
__ 5. Modify the Target Network Manager Host, SNMP Port Number and Community as appropriate for your environment.
__ 6. Set the remaining Send Trap fields to TRUE for each notification type you want to receive at the SNMP target host.
__ 7. Click OK.

**How to add an Email alert**

__ 1. Select a monitored machine for which you want to create an Email alert folder. (Email Alert is common for all the SA clients on the same gateway, irrespective of where we add the Email alert mechanism)
__ 2. Click **Add**.
__ 3. Click **Child sub-menu**.
__ 4. Click **Email alert**.
__ 5. Change the default e-mail address to whom you want to send the e-mail to. You can send an alert to multiple e-mail addresses by separating the e-mail addresses with a comma. For example, joe@host.companyname.com, carol@abcit.com, jill@companyname.com .
__ 6. If the selected host has a different Mail Server, type the name of that server as the value for Email Server.
__ 7. Change the *Email Wait Time in Minutes* field to something quicker than 15 if you want to check the function or receive notification sooner. You can not use a value of 0.
__ 8. Set to **True** the types of alerts of which you want to be notified. For more information and a description of the alert types, refer to *Appendix A "Advanced Configuration Details - Email Alerts"*.
__ 9. Click **OK**.

**Note**: Different Email alerts can be customized for particular users. For example, you may want employee A to be notified of CAUTIONS and employee B to be notified of INTERNAL ERRORS. Only one Email alert is normally needed for any events which might happen on any of the systems using this gateway. Adding Email Alerts to individual nodes, does NOT provide details specific to that nodes.

## How to remove or delete configuration entries

**How to remove a machine**

__ 1. Select **Network** property.
__ 2. Select the **machine** to remove.
__ 3. Click **Delete**.
__ 4. Click **Yes** to complete the removal.
**Note**: This only removes the client Hardware Management Console from the Service Agent configuration.

**How to remove any Item from a machine**

__ 1. Select **Network** property.
__ 2. Select the **machine**.
__ 3. Select the Item to remove. ( if item is removable then Delete will highlight )
__ 4. Click **Delete**.
__ 5. Click **Yes** to complete the removal.

**How to remove a SNMP Notification**

__ 1. Select the **Network** property.
__ 2. Select the **machine**.
__ 3. Select the SNMP Notification you want to remove.
__ 4. Click **Delete**.
__ 5. Click **Yes** to complete the removal.

## How to test certain configuration entries

### How to send a test PMR to the IBM

__ 1. In the Test Tools folder, click **TestPMR**.
__ 2. Select a *machine* and click **Generate** to create and send a test PMR to the IBM.
__ 3. Reply Yes to the prompt of whether to connect to IBM now or later.
__ 4. Click the **Calllog** property to monitor the PMR progress for success or failure.
__ 5. Look in PMR folder beneath the monitored machine property. It should be a Red bug icon prefaced by the error string 000-000.

### How to send a test SNMP Notification

__ 1. Select the Test Tools.
__ 2. Click Test SNMPTrap.
__ 3. Click Generate.

### How to send a test Email

**Note**: You have to have an Email alert defined prior to sending a test e-mail. See *How to add an Email alert* in the above example.

__ 1. Select a monitored machine for which you want to create a Test Emails folder. You must expand the view of the monitored machine by clicking the key to the left of the machine name.
__ 2. Click **Email alert icon**.
__ 3. Scroll to *Test Emails Enabled* field.
__ 4. Click the **Test Emails Enabled** check box to toggle the value to True.
__ 5. Click **OK**.
__ 6. Repeat steps 1 through 5 to send test e-mail's to other e-mail addresses.
__ 7. Expand the **Test Tools** property.
__ 8. Click the **TestEmail** icon.
__ 9. Click **Send**.
**Note**: E-mail is sent after the time-delay (set when created the e-mail alert) expires.
__ 10. Scroll (while in the Email folder) to *Test Emails Enabled* and click the **Test Emails Enabled** check box to toggle the value to False.
__ 11. Check with the person(s) who are designated to receive the e-mail alerts to see if they did receive the alert(s).
**Note**: The e-mail test alert instructs the recipient to contact the system administrator.

## How to perform other Service Agent functions

### How to determine your Service Agent version

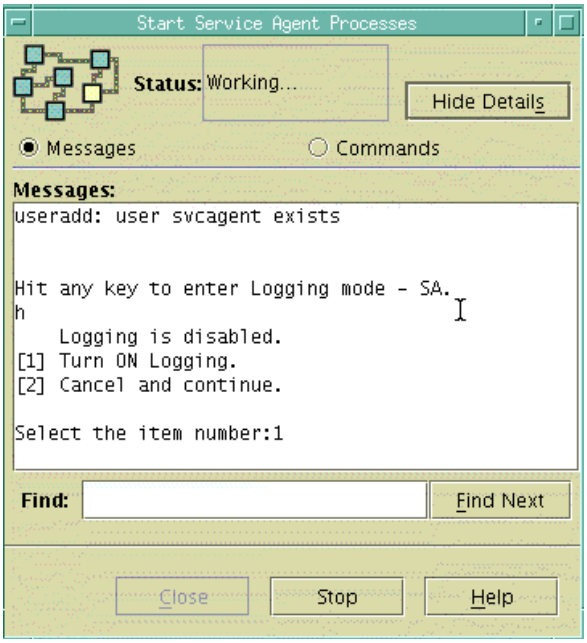
__ 1. From the Service Agent interface, click **Help**.
__ 2. Click **About**.
__ 3. About displays the Service Agent version number on the SA splash window.
**Note:** This displays the level of code installed on the Gateway server. Selecting the Environment item under the expanded node shows the Service Agent code level for that machine.

**How to send Vital Product Data (VPD) to IBM**

__ 1. From the Manual Tools folder, click **VPD**
__ 2. Select a *monitored machine* for which you wish to send VPD.
__ 3. Click **send VPD**.
Send VPD sends VPD to IBM at the next regularly scheduled time.

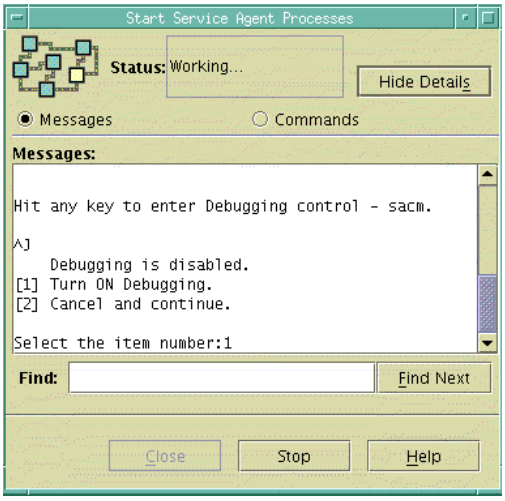
**How to Activate Logging on SA**

__ 1. From the WebSM Service Agent menu
__ 2. Select *Stop Service Agent Processes* and verify working menu is successful.
__ 3. Select *Start Service Agent Processes* and be ready to press any key to go into logging.
__ 4. When working window is displayed with detail messages.
- Select focus to the working window by clicking on window.
- When you see prompt to enter Logging mode.
- You have a few seconds to press a key to enter logging mode, else process will




continue.
- Current status of Logging is displayed. In this case Logging is disabled.
- Enter a 1 to turn on Logging
- Enter a 2 to continue without changing any settings if Logging was enabled.

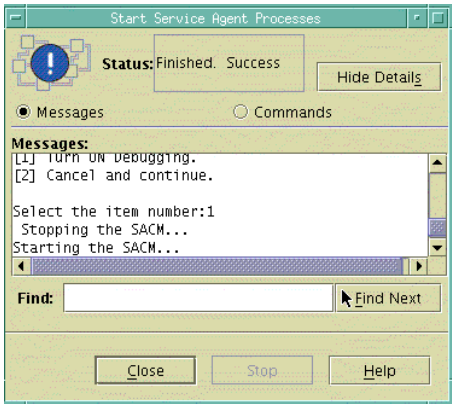
__ 5. Once you hit enter, the process will allow you to activate Debug on SACM.
- You have another delay to press any key to enter Debug mode, else process will continue




- Enter a 1 to turn on Debugging
- Enter a 2 to continue without changing any settings.

__ 6. Once the data is entered the process should go to completion without any additional intervention.

__ 7. You may close the window if Finished Success.




**How to Activate Debug mode on SACM**

__ 1. From the WebSM Service Agent menu

__ 2. Select *Stop Service Agent Connection Manager* and verify working menu is successful.

__ 3. Select *Start Service Agent Connection Manager* and be ready to press any key to go into Debug.

__ 4. When working window is displayed with detail messages.
Reference the above images of the previous “How to” for SACM Debug mode.

- Select focus to the working window by clicking on window.
- When you see prompt to enter Debug mode.
- You should have a 10 second delay to press any key to enter Debugging mode.
- Enter a 1 to turn on Debugging
- Enter a 2 to continue without changing any settings.

__ 5. Once the data is entered the process should go to completion without any additional intervention

__ 6. You may close the window if Finished Success.

**How to Create a PMR**

__ 1. From the Manual Tools folder, click **PMR**
__ 2. Select a *monitored Hardware Management Console machine* you wish to use.
__ 3. Click **Generate**
__ 4. A window will appear with all machines managed by the selected Hardware Management Console.
__ 5. Select the *managed machine* for which you wish to create a PMR against.
__ 6. Click **OK**
__ 7. Change the default 000-000 to desired error.
__ 8. Fill in the required *Description* and *Error Details* fields.
__ 9. Pre-filled fields should be OK, and only **Hardware** PMRs can be created.
__ 10. Click **Generate**
__ 11. Select immediate or delay with the **YES No** options for call queuing.

**How to cleanup (remove some data from) monitored logs**

You may want to clean up logs if they are getting too large or you only want to keep certain data.

__ 1. Expand the **Administration key**.
__ 2. Select **Purge Data**.
__ 3. Toggle to True the data you want to purge:
- CallLog data
  All entries posted to the CallLog. For example, when a call is made to IBM, a record is created in the CallLog. This function removes ALL data in the CallLog.
- Purge Error Warning
  Any warning messages (non-error messages (yellow triangles)) are purged.
- Purge Internal Errors
  Any errors with the upside-down Red Bug icon posted beside them are purged.
- Closed PMRs
  Purges any PMRs marked as closed.
- All The PMRs
  Purges all PMRs.

__ 4. Click **Purge** to purge all data marked as True.
**Note**: If there is a large quantity of data to purge, this activity could take some time to complete. You will not see any screen updates while this activity takes place.

**How to clear pending request to the IBM Service Data Receiver**

Normal workings of Service Agent can create request to the SDR. They can be queued for immediate or later processing. To clear any current or pending request follow the steps below:

__ 1. Click the **Administration** property folder.
__ 2. Click **Purge**.
__ 3. Toggle **The OutGoing Queue** to True.
__ 4. Click **Purge**.
**Note**: You will not see any screen updates while this activity takes place.

**How to do a Clean SA install**

Sometimes there is a need to restore SA database to original data or start from a clean SA configuration. This might be due to a forgotten password or a corrupted SA database. Here are a couple of methods to clear SA database without loosing the customers critical data.

- Method 1 without having access to root authority, save backup data without including SA data.
  __ 1. Stop all SA daemons, Gateway and Connection Manager.
  __ 2. Check that no SA daemons are running.
  __ 3. Use HMC process to save or backup customer critical data.
  __ 4. Restore HMC firmware from upgrade or recovery DVD.
  __ 5. Restore customer critical data from step 3.
  __ 6. After HMC reboot, SA should still be stopped and should have to be initialized from scratch.

- Method 2 access to root authority, obtain daily password from PE.
  __ 1. Restore HMC firmware from upgrade or recovery DVD.
  __ 2. Save "/var/svcagent/saspace/saspace.img & saspace.jrl files to /tmp.
  __ 3. Restore customer critical data
  __ 4. Restore the SA image and journal files saved in step 2 from /tmp.
  __ 5. After HMC reboot, SA should still be stopped and should have to be initialized from scratch.

# Service Agent Security

This chapter discusses how security for Service Agent works with the following areas:

- IBM Service Data Receiver using HTTPS
- SA Connection Manager
- Global Dialer and Network
- Modem security

Access to the latest Service Agent security information resides on the following URL:
**www.ibm.com/support/electronic**

- Select a **Country**
- Select **Electronic Service Agent ™**
- Under **Resources** expand General information
- Select the latest security information document you wish to review

## Traversing Secure Boundaries

An Inter-Enterprise Service (IES) activity is the IT process of providing access to proprietary IT Resources. In providing that access the secure boundary of IT infrastructure must be traversed. Each communication path brings its own security requirements.

The SA application was re-engineered to be IES compliant. It will now utilize an HTTPS connection to the IBM SDR. This IES compliance function to utilize the SDR will be integrated into both the pSeries Standalone AIX release and Hardware Management Console release.

The Service Agent Connection Manager will support a https connection to the SDR. Since both the Service Agent gateway implementations (Standalone and Hardware Management Console) are coded in Java, the Java Secure Socket Extension (JSSE) package will be used.

The SA Gateway will need to provide the SDR all the information it knows about a given system during enrollment. This information can be pulled from the Node Info associated with the machine in question. This applies to both methods now being used by SA, the Internet or the Dialer.

### Global Dialer networking to IBM SDR

The purpose of this is to provide an overview of the security methods in place for the AT&T account SA uses. Please follow the URL access to see AT&T *IP Remote Access Dial Security* document.

### Understanding Serial Interface

The stty port and modem security are both configured to *not* auto-answer the modem or allow login access from the stty port. Service Agent only allows outbound calls to be created from the customer's location.

# Appendix A. Configuration details

This appendix describes the details of the Advanced Configuration folders, templates, template parameters and their fields.

This information is presented in the order you view the Advanced Configuration user interface.

- Network
- Gateway Hardware Management Console server
- Monitored Client Hardware Management Console
- Administration
- Filtering
- Manual Tools
- Test tools

## Network folder

The Network folder allows you to update the contact information for callback from the IBM Service Center for problems that are received. The *Name, Phone Number*, and *Email* address of the contact are required. In addition, the *Queue Country* where the Gateway server is located is also required. After the data has been typed, click **OK** to save the data.

**Note**: The country value selected is utilized to properly identify the systems and open Problem Management Reports (PMRs) based upon internal country codes. The country selected must match with the IBM customer number. If the Country code is incorrect, the PMR is either rejected or sent to an improper queue.

**See:** Telephone Number if network dispatch is different from required Contact Phone Number line 2, this will allow proper dispatch.

**Network Template**:

| Parameters | Description |
|---|---|
| | |
| **IBM Contact** | Customer, IBM Support May Contact |
| ! Name | Name of a person IBM may contact for PMR discussions. (Required) |
| ! Phone Number | Phone number of contact. (Required) |
| ! Email | Email address of contact. (Required) |
| **eService Information** | |
| IBM Common Registration UserID | Your IBM account registration user ID, used to view machine information that was delivered to IBM SDR. If this field has a valid ID during enrollment the machine will automatically be associated with the ID. |
| **Address** | |
| ! Queue Country / Region | Physical Country Location of the systems that PMRs will be open against. This will generally be the same country the contact person resides in. However, if different the country where the Service Agent network is located should be used. (Required) |
| Organization | Name of company. (Optional) |
| Organizational Unit | Name of group or division (Optional) |
| Street | Street location where SA is installed. (Optional) |
| Locality | City, Town, or Village where SA is installed. (Optional) |
| State Or Province | State/Province where SA is installed. (Optional) |
| Postal Code | Zip or postal code where SA is installed. (Optional) |
| **Customer** | |
| Customer Number | IBM customer number. (Optional, wrong number may cause problems). |
| **Standard Template Settings** | Default Template settings use across all monitored systems. |
| Err Lease in Days | This timer determines how long to keep and maintain host detected error entries within Service Agent database. Default=30 |
| **Contact Context** | |
| Comment | Any comments that may help in communication between the company and IBM concerning support for the Service Agent monitored systems. |
| **Telephone Number** | **Additional Phone number for local informational purposes. This will override the primary contact phone number for call back proposes. This number should be a number located where the machine is located. If different from the Primary number.** |
| Number | Will override the primary contact phone number entered above |
| Additional Entries | Additional data may be added to this folder with the use of Add-Form |
| Forms | Location, Threshold, Filter, additional comments, contacts, addresses will reflect as Tab entries on base form. |

## Using the Add button from the Network folder

When the Network folder is selected you can add additional information about your Network to the Service Agent program using the *Add* button. This additional information can be viewed, through the Network folder's details list.

**Node Info template parameters and descriptions**

- Select Add
- Select Child
- Machine

The selection of Machine under the Child option of the Add function will allow you to add Client Hardware Management Console machines to your SA Network. The Node Info template allows you to define specific information about new Hardware Management Console that you want to add to the network of monitored machines. The following table defines and describes the parameters:

**Node Info**

| Parameters | Description |
|---|---|
| ! Name | Enter the fully qualified hostname of the system to be added. This is the Hardware Management Console hostname the Gateway Hardware Management Console will see it as. |
| IP address | If entered must be in proper IP number format ###.###.###.### |
| Processor ID | (ProcessorID) of the Hardware Management Console machine, should auto fill. |
| ! Type | Required input- 4 digit brass tag number located on the exterior of the primary Hardware Management Console controlled CEC. (eg. 7040) |
| ! Serial Number | Required input - Last seven characters of the brass tag serial number located on the primary Hardware Management Console controlled CEC. (In United States use 00 for plant code.) |
| ! Model | 3 character model number of the primary Hardware Management Console controlled CEC. |
| Manufacturer | (Optional) Manufacturer of unit. (e.g.. IBM) |
| InstallationType | **N/A**, SA Code is not distributed within the Hardware Management Console Network. |
| Primary Server (Locked) | Used for internal functions within Service Agent for Gateway and sub-host communication. Indicates primary host, that sub-host reports to (may have to be fully qualified name). |
| Secondary Server | (This functions currently not active) |
| Tertiary Server | (This functions currently not active) |

Client Hardware Management Console could have been added under a Department sub-grouping by first building a department using Add-Child-Department option. Prompt to enter a department Name and save it by clicking the OK, Cancel will return with no action taken to the database.

**Adding additional system information using forms**

Additional information may be added to a Network, Department, or Node by selecting the Add button and then the Form button at the bottom of the navigation pane and making a selection.

The following selections may take affect across the whole network hierarchy, department or on an individual machine basis, depending upon the Property selection made. Forms added to a Machine take priority over a Department grouping and Forms added to a Department take priority over the Network.

**Available Forms:**

**Address**
Select the *Address* form to add additional address information to the Network, Department, or Machine.

**Comment**
Select the *Comment* form to add additional comment information to the Network, Department, or Machine.

**Contact**
Select the *Comment* form to add additional comment information to the Network, Department, or Machine.

**Location**
Select the *Location* form to add additional location information to the Network, Department, or Machine as to the physical location of the system. Specific entries available are Building, Floor, and Room location.

**Resource Filter**
You can define resources for which you do not want to report errors. For example, a hard disk that is not under an IBM warranty or maintenance agreement. Generally, resource filters are defined at the machine level but they can also be set at the network and department level. Enter the logical resource name of the device to be ignored. Add one resource form per device or range of devices. For example, ("hdisk0, hdisk1, tok0, tok1"). See Chapter 5 for more information on how to define resource filters

**Telephone Number**
Select the *Telephone Number* form to add additional phone number information to the Network, Department, or Machine.

**Threshold**
Select the *Threshold* form to add additional error thresholds to the Network, Department, or Machine. Error events detected by Service Agent use internal threshold levels, defined by IBM, that must be exceeded before an action is taken (Ignore, Create Pending, or Create Held). In some cases, false error events may be detected due to system configuration or unusual process activities which give false returns. If this happens, thresholds can be added for the specific error Thresholds Property Selection

**Available Threshold Entries:**

| | |
|---|---|
| **Error ID** | The Error ID can be a SRN number generated by the Diagnostics, a system error log error identifier, or a system error log error label. The Error ID or SRN number will be displayed in the "Error Number" field of the "Error Event" if available.<br>**Note:** A threshold Error ID or SRN must be an exact match. If the Error ID detected by Service Agent contains upper or lower case characters the same characters must be entered for the thresholds. All characters displayed in the Error ID of a PMR entry must be typed as the Threshold error. This would include any hex notation such as *0x* if present. |
| **Action** | Action to be taken when this error occurs: |
| CREATE PENDING | Create error event to be transmitted to IBM |
| CREATE HELD | Create an error event with Held status so it does not get sent to IBM. You would then have to manually change the status to Pending to send it or delete it if you were not interested in it. |
| IGNORE | Ignore this error completely; do not report it. |
| Count | The number of occurrences of the error before the action is taken. |
| Days/Hours/ minutes | The frequency of the count; for example, you might only want to act on the error after it happens 3 times in 1 day, or 2 times in 45 minutes. |

## Gateway folder templates

**Node Info template**

| Parameters / Fields | Description |
|---|---|
| **Node Info** | **Same as Network level** |

**PMR folder** 

When Service Agent receives a valid Error Event it puts the event in a template within a PMRs folder beneath the host (as viewed using the Service Agent interface) it was reported on. The information defined in this template is used to open a PMR and to maintain its returning status and PMR number. When viewing an expanded machine Error Event, templates are indicated by an icon in the shape of a bug along with the SRN or error number of the event and its description. Selecting an individual error template displays its contents in the detail pane to the right. These entries are removed when the "Err Lease" value specified in the detail pane of the "Network" selection is reached.

If the View Error Events icon is selected and the machine is selected all of these events will be displayed in a summary list. Selecting an event will show details on bottom of view pane.

| PMR | Description |
|---|---|
| Timestamp | Time stamp when Error Event was first created |
| PMR Number | Problem Management Report (PMR) number returned from IBM. |
| Status | This field depicts the current status of the Error Event and the results of the PMR request. This field can be set to any of the entries in the status table.<br>**0 Pending** This status indicates an entry that is set to be sent to IBM. It is the initial status state which triggers the Service Agent CallController to connect to the IBM SDR. If the status is some other state, setting it to Pending again causes the entry to be resent.<br>**1 Open** This indicates a PMR was opened in the IBM support center for this machine.<br>**2 Closed** This indicates a PMR was closed in the IBM support center for this machine.<br>**3 Held** This status indicates the Error Event entry was held. No connection to IBM was made for this status state.<br>**4 Duplicate** This status indicates an attempt was made to open a PMR that was already opened. If the same Type, Serial number, Description, and error number is opened before a previous PMR with the same error is closed a Duplicate status is returned.<br>**5 Failed** This status indicates an attempt to open a PMR with IBM failed for some reason. See the Status Details field for specific details on the error. |
| Error Number | The Error Number is the actual error number found in the error log or the SRN number generated by the concurrent diagnostics on the machine. |
| Description | This is the short verbal description of the error indicated from the system error log or the diagnostic data files. |
| Resource | This is the name of the resource the error occurred on. |
| Duplicate Count | This count indicates how many times the error has occurred since it was originally opened. See **note** following chart. |
| Last Occurrence | This is the time stamp of the last occurrence of the Error Event. |
| Error Details | This field contains the detail description of the Error Event that occurred. This data will all appear in PMH record in RETAIN. |
| Status Details | This field contains the detail description of the status results. If the status is set to FAIL due to some communication problem with the SDR this field would contain the associated error message. |
| whenStatus Checked | Last time the status of an opened PMR was checked. |
| errClass | Classification of the PMR. |
| Type | The machine type the error was posted against. |
| Serial | The machine serial number the error was posted against. |
| Model | The machine model the error was posted against. |
| Cluster Type | Valid cluster type if machine is part of a cluster environment. |
| Cluster Serial | Valid cluster serial number if machine is part of a cluster environment. |
| Cluster Model | Valid cluster model if machine is part of a cluster environment. |
| Partition | Number of the reporting partition. |
| Partition Name | Name of the reporting partition. |
| Special Handling | Will list any valid special handling information for this machine. |
| Country Code | Country code if needed for this machine. |
| Branch Number | Branch office number if needed for this machine. |
| Internal Problem Number | If internal problem numbers are assigned to the PMR, it will be posted here. |

**Note**: Duplicate Count -- Every time a duplicate error occurs, a check is made to see if the original creation date of the OPENed PMR is greater than 24 hours. If so, then the local status of the PMR is set to *PENDING* and an attempt is made to contact IBM again. If the PMR was closed at IBM, a new PMR number will be generated replacing the original one. If the PMR is still open, then the local status will be reset to *OPEN* and the original PMR number will be maintained For tracking purposes the original PMR number is appended to the details text of the PMR when the PMR is replaced.

**Environment template**

The Environment template displays the various environment and revision levels of the supporting system and execution files on the machine. The revision levels information is gathered every time the ODS process is started on the machine. The Environment information is transmitted with each connection to the IBM SDR for error analysis and update notification. These entries are locked and cannot be modified.

| Parameters / Fields | Description |
|---|---|
| java Vendor | The Java builder running on Hardware Management Console, usually IBM Corporation |
| java Version | The Java level running on Hardware Management Console |
| Operating System | Linux is the operating system running on Hardware Management Console currently |
| OS Version | The build and level of operating system |
| System Architecture | Architecture of system running Hardware Management Console |
| Language | Language environment setting on Hardware Management Console |
| Service Agent Version | The release, version, and fix level of SA running on this Hardware Management Console |
| Service Agent Type | Type of SA running on this Hardware Management Console, ( HMC vs AIX or Linux) |
| Lockout | If set to True, SA is effectively disabled on this Hardware Management Console |
| Logical Partition | The logical partition number assigned to this Hardware Management Console host |

**Enrollment folder**

List of available machines supported by this Hardware Management Console which show the enrollment status of HMC and supported CECs. The CEC Objects will be shown as MOB Type.

**Enrollment Object template**:

| Parameters | Description |
|---|---|
| Machine Type | CEC machine type, information from SFP. |
| Serial Number | CEC serial number, information from SFP. |
| Model | CEC model, information from SFP. |
| Logical Partition | The LPAR number assigned to this CEC. |
| Service Agent Type | This will always be HMC or MOB (CEC assignment). |
| Enrolled UserID | The assigned userID for enrollment access. |
| Comment | Special comments section. Contains latest Enrollment date and results. |
| Hostname | Host name assigned to the enrollment object. |
| Operating System | OS that is running on that object. |
| OS Level | Level of the running OS on that object. |

**CEC folder**

List of available machines supported by this Hardware Management Console which have VPD, LPAR status, or MicroCode information posted. Select the available Type_Serial_Model machine that you wish to review. The CEC template will be displayed with all fields locked available for viewing only. If the "Resource is Active" is checked as True, then the associated VPD data or Microcode information may be reviewed from their respective scroll bar windows on template

**VPD & Microcode template**:

| CEC Parameters | Description |
|---|---|
| Machine Type | The value of this parameter will be from information from SFP. |
| Serial Number | The value of this parameter will be from information from SFP. |
| Model | The value of this parameter will be from information from SFP. |
| Host Name | The value of this parameter will be from information from SFP. |
| Resource is Active | Will reflect the active state of this partition information. |
| Vpd Output Format | The format that the VPD file will be in. (invscout) |
| Vpd Output Status | The actual VPD file, will have scroll bar if required. |
| Vpd Output FileName | The path and filename of the actual data file on SA gateway machine. |
| Microcode Output | Any pending microcode files pertaining to this host. |
| LPAR Status | Current Status of this listed host logic partition. |

**Dialer template**

The dialer template allows you to define the modem parameters and field values for communication to the IBM SDR. In this template, required fields are marked by the "!" character as in other screens within Service Agent. However there is no verification of required fields for the modem parameters since a modem is not required for local setup of the rest of the Service Agent program. The dialer comes into play when you are ready to enroll the systems and open problem reports (PMRs) and send them to IBM automatically and you do NOT have an Internet connection available.

**Dialer**

| Parameter | Description | |
|---|---|---|
| Location | The country/city the modem is calling from. By opening this table and selecting the country then clicking Details the local country data will be displayed. Highlight the town closest to your location, and press the Select pushbutton. Additional fields are automatically filled in if available.<br>Some countries may have a nationwide or a fee-based 1-800 number available to use. If a local location number from the Location table is not available, look under Nationwide or Fee for a possible toll access number to use instead of a number from the Location table. | |
| Primary Phone Number | The phone number the modem uses to call out is populated according to the location selected. Change this phone number only if needed.<br>**Note**: Depending upon the local phone exchange, this number may need to be modified to utilize your outgoing number and area code requirements. | |
| Location | The country or city the modem is calling from for additional dial attempts if primary should fail for configured maximum attempts. Use same procedure as for primary. | |
| Secondary Phone Number | The phone number the modem uses to call out in the event the primary phone number fails.<br>**Note**: Depending upon the local phone exchange, this number may need to be modified to utilize your outgoing number and area code requirements. | |
| Account | The Service Agent network login account assigned by IBM. May vary depending upon Location. Will be **automatically** filled with valid phone number selection. | |
| User ID | The Service Agent network login user ID. Will be **automatically** filled. | |
| Password | The Service Agent network login password. Will be **automatically** filled. | |
| TTY # | The port number the modem is physically connected to (0,1,2,3) (ttyS1 for com2 on Hardware Management Console) | |
| Modem | The modem's reset and initialization string values are populated according to the modem selected. Change these values only if needed.<br>**Tip:** Type the first letter of the modem to move quicker through the list. | |
| Baud Rate | The maximum value the TTY modem will be set at for connection: | |
| | | 19,200 |
| | 1,200 | 28,800 |
| | 2,400 | 33,600 |
| | 4,800 | 38,400 |
| | 9,600 | 57,600 |
| | 14,400 | 115,200 |
| Reset String | The modem's reset string values are populated according to the modem selected. Change these values only if needed. | |
| Init String | The modem's initialization string values are populated according to the modem selected. Change these values only if needed. | |
| Dial Type | Select the dial type of this modem ( tone or pulse). | |
| Max Retry Attempts | This value determines how many attempts to make a connection to the IBM SDR before giving up and setting the **PENDING** status of the events to **FAIL** and clearing the call queue. | |
| Retry Timer in Seconds | This value determines how many seconds to wait before making the next connection attempt. | |

**CallController template**

The CallContoller template contains the entries and timers used to coordinate the call notification attempts among the monitored machines when an event or error is detected. The Call Controller will direct the assigned Hardware Management Console Gateway request to the master or secondary Connection Manager.

| Parameter | Description |
|---|---|
| Primary URL to Connection Manager | This entry determines the address and Port number of the Connection Manager. This value normally localhost:1198 which is the loopback when the SACM is on the same host. But if Master Connection Manager is on a different host then this would point to that host fully qualified hostname or IP address and port 1198 |
| Secondary URL to Connection Manager | This entry determines the IP address and Port number of the backup or secondary SACM server. This option can also point a different host Connection Manager to provide redundancy or secondary modem or Internet connection. |
| Pending Timer in Minutes | When an event or problem is detected its status is set as Pending. The value specified for the Pending Timer determines how many minutes to wait for additional events to be generated before taking action and attempting to make a connection to the IBM SDR. For example if an error is detected at 1 PM, Service Agent will wait until 1:15 PM before calling out to IBM and placing a Problem Management Report. |
| Check Open PMR Status in Days | When an error event is set to an OPEN status the value specified in this field determines how many days to wait before checking the status of the PMR on the SDR server side. When the PMR is closed at IBM the local status is updated. |
| Health Check Timer in Days | The value specified in this field determines how often (in days), Service Agent should call into the IBM SDR for a health check. It indicates that everything is OK and the reason SA hasn't called in before is because there were no errors to report. SA will automatically connect to the SDR, if it hasn't done so for some other reason, when the time specified expires. Whenever a connection is made to the SDR the countdown for this timer is reset in order to keep outgoing connections down to a minimum. |
| Max Call Home Retry Attempts | This value determines how many attempts to make a connection to the IBM SDR before giving up and setting the **PENDING** status of the events to **FAIL** and clearing the call queue. |
| Retry Attempts Counter | This value indicates the current connection attempt the CallController is on. When this count equals the Max Attempts count., the Entries in the Call Queue are set to FAIL and the queue is cleared. |
| Retry Timer in Minutes | This value determines how many seconds to wait before making the next connection attempt. If the Max Attempts is set to 3 and the Retry Timer is set to 5, then the CallController sleeps between each attempt for 300 seconds until the Max Attempts value is reached. |
| Connection Idle Timeout in Minutes | This value determines how long a connection can be idle (no activity) before a time-out condition is posted back to the CallController and breaking the connection to the Connection Manager. Default 5 hours |
| Proxy IP to Connection Manager | This entry determines the IP address for the proxy server if the Connection Manager is behind a firewall and a proxy server must be used to access SACM host. |
| Proxy Port to Connection Manager | This entry determines the Port number for the proxy server if the Connection Manager is behind a firewall. Default = 80 |
| Proxy Username | If proxy server requires a user name for access, enter that user name here. |
| Proxy Password | If proxy server requires a password for access with that user, enter the password here. |
| Use Socks Proxy | Set to True if you must use Socks Proxy. Default is false |
| Download Connection Manager Configuration Timer in Hours | How often the CallController will retrieve the Connection Managers Configuration, to make sure the SA Gateway has the matching configuration for database image. |

**Available buttons for CallController template:**

| Button | Description |
|---|---|
| OK | This button located at the bottom of the detail pane is active once data has been entered or changed in a field. Click this button to save all data. |
| Cancel | Click Cancel to cancel the current operation. Screen is refreshed to original data. |
| Delete | This button, located at the bottom of the detail pane, becomes active when an entry in the detail pane is selected. Click the Delete button to delete a selected entry. |

**Connection Manager template**

The Connection Manager template contains the entries and timers used to coordinate the call attempts to IBM SDR. There may be more than one Connection Manager for an account complex under the Network configuration primary is usually under the SA Gateway host. A secondary CM may be configured on another SA Client host on the same Network. The applied CM configuration is controlled by the setting of the CallController URL to the CM settings.

**Connection Manager:**

| Parameter | Description |
|---|---|
| Use Modem as a Connection Method to IBM | This check mark when set to true will use the dialer to contact IBM SDR. When set to false will expect to use an existing Internet connection. |
| Password for updating ConnectionManager configuration | Password to validate SA Gateway, must match the CfgUpdatePassword in svcagent/cfg/sacm.cfg file. default = password |
| Proxy IP to SDR | (leave empty if no proxy) |
| Proxy Port to SDR | default port = 80 |
| Proxy Username | (leave empty if no user name) |
| Proxy Password | (leave empty if no password) |
| Timeout for connecting to SDR in secs | The maximum time allowed to make connection to the SDR. default is 2 minutes |
| Read Timeout for SDR in secs | This is the maximum wait time for a read operation to be started. default is 30 minutes or 1800 sec |
| ChunkSize for data from ConnectionManager to Sdr in bytes | The data block size of transmitted information default = 4080 |
| Delay between Chunks from ConnectionManager to Sdr in millisecs | This is the number of milliseconds to wait between data blocks. default = 0 |
| The interval for the gateway monitor process on ConnectionManager in mins | How ofter the SA Gateway will check SACM process. default = 2 |
| The size of the log for ConnectionManager in KB | Set the max size of SACM log in KiloBytes. default = 2048 |
| Interval for the check for update to configuration files on ConnectionManager in mins | How often SACM should the ESS database for any changes to the Connection Manager configuration. default = 30 |
| Dialer keep alive in secs | Interval for maintaining the dialer connection to prevent time outs. default = 120 |
| Minimum Gateways allowed to connect to ConnectionManager | This is the minimum number of SA gateways, always should be one (1). |

| | |
|---|---|
| Maximum Gateways allowed to connect to ConnectionManager | This is the maximum number of SA gateways that can connect concurrently to Connection Manager to utilize its call path. (10) |
| Number of Gateways to be queued | This is the maximum number of SA gateways that can queued to Connection Manager if all available connections are busy. |
| ChunkSize for data from ConnectionManager to Sdr in bytes | The data block size of transmitted information.<br>default = 4096 |
| Wait Timeout for Gateway in secs | This is the time out value in seconds., the default is 2 minutes. This should be set for less than the socket time out on a gateway. |
| Read Timeout for Gateway in secs | This is the maximum wait time for a read operation to be started. default is 2 minutes |
| The length of time the gateway connection can be alive in mins | This is the maximum time of SA gateways can maintain any one connection. So every 5 hours the connection must be released. |
| The URL for SDR | The complete secure URL definition for the IBM Service Data Receiver. |
| The backup URL for SDR | The complete secure URL definition for the backup IBM SDR. |
| Use Socks Proxy | Set to true is you must use proxy to access IBM. default = false |

**Available buttons for Connection Manager template:**

| Button | Description |
|---|---|
| OK | This button located at the bottom of the detail pane is active once data has been entered or changed in a field. Click this button to save all data. |
| Cancel | Click Cancel to cancel the current operation. Screen is refreshed to original data. |
| Delete | This button, located at the bottom of the detail pane, becomes active when an entry in the detail pane is selected. Click the Delete button to delete a selected entry. |

**Linux Hardware Service template**

| HMC SA Service Settings | Description |
|---|---|
| Status | This entry displays the enrollment status of the hardware template. This entry could be one of seven different status states.<br>0 proposed -<br>This state is the initial default state of a newly define machine. It indicates the system is only proposed and not enrolled. No action will be taken until the status is set to Pending.<br>1 pending -<br>This state indicates the system is staged to be licensed. Upon the next connection to the IBM SDR an enrollment request will be made for this host.<br>2 expired -<br>This state indicates the maximum enrollment date has passed and the enrollment is expired. Reregister the system to get a new enrolled status. Enrollment functions are disabled. When a system is expired Service Agent automatically connects and requests a new enrollment. |

| | |
|---|---|
| | 3 corrupt -<br>This state indicates the enrollment status is corrupt or damaged. For example if the SA key is modified the status will be set to corrupt. Reregister the system to get a clean enrolled status. Enrolled functions are disabled with this status.<br>4 enrolled -<br>This state indicates the machine is enrolled. All functions requiring a enrollment are activated.<br>5 denied -<br>This state indicates the system was denied for some reason and enrollment to activated this template is refused. All functions requiring enrollment are disabled. Refer to the template comment field or the specific calllog entry for details. You must remove and redefine the machine to remove the denied status state.<br>6 failed -<br>This state indicates the enrollment attempt failed. For example if the return from enroll request was a bad transmission the status will be set to failed.<br>If the template is not enrolled, those functions requiring licenses are not run. Functions requiring a licensed status are the hardware monitoring functions. |
| Expiry | This is the date the enrollment expires. |
| SA Key | This the unique enrollment number associated with the machine. This enrollment number will not work with any other defined host. |
| Comment | General status response comments from IBM SDR. |
| Heart Beat | Heart Beat is always enabled. Shows ODS process is running and in communications with the ESS process. |
| Days / Hours Minutes Seconds | Timer to determine how often the gateway should expect a heartbeat from the host. If the host misses a heartbeat a notification is sent if Email alert is set. Actual time is an approximate value of HeartBeat + Delay. |
| Heart Beat Delay in Minutes | Value added to the Heartbeat to compensate for Network delays and differences in systems. Minimum value is 2 minutes. |
| Vpd Enabled | Enables or disables Vital Product Data (VPD) collection.<br>True value indicates Enabled. |
| Vpd Interval | This timer determines how often to check for Changes in the Vital Product Data on a host. This data is then transmitted to IBM SDR. Days, Hours, Minutes, Seconds |
| Create Internal Err for Unformatted Events | Flag to determine if Event comes from Service Focal Point without proper formatting. This will then be logged as an internal SA failure. Enabled if checked True |
| Error Enable | Flag to determine if the error events from SFP will be sent to Service Agent. The Hardware Template must be enrolled for this to be active. |
| Error Interval | This timer determines how often to check for errors or problems.<br>- Days, Hours, Minutes, Seconds |
| Enable the Automatic transmission of EED | Flag to determine if the EED will be automatically transmitted with error events. Enabled if checked True. |
| Update CEC List Interval | This timer determines how often to check for updates to CEC list.<br>- Days, Hours, Minutes, Seconds |

**Performance Management folder**

**Note:** The IBM Performance Management for AIX product must be installed on each machine (or each LPAR) for Service Agent to pick up the performance data through the Hardware Management Console SFP connection of the LPAR and send to IBM.

The *IBM Performance Management For AIX* product, installed on the AIX system, gathers and creates data files for the following system activities:

- Disk usage; a summary of disk usage of physical volumes and space on the file system
- IO data; Input/Output statistics for disks and CD-ROMs
- Networking data; network statistics for defined interfaces
- Virtual memory and CPU statistics

The Performance Management module in Service Agent on the defined Hardware Management Consoles helps to gather the data from the monitored systems. It will trigger the request if the "Enable gathering of PM about this system?" is set to true at time of day to collect setting shows. The SFP will obtain the daily send files and sends the data to the Hardware Management Console Gateway machine. The SA Gateway machine will then compress the data file and rename it to assigned CEC MSMT and then send the file to IBM SRM for WEB viewing.

**PMData folder**:
This folder will contain the PM data files from the time they are collected until they have been successfully delivered to the IBM SDR. So if folder is blank that means no data files are outstanding. Once first data file is received by SA database from the Hardware Management Console SFP interface a pending request to transmit is started.

**Note:** AIX SA Client code does not have to be installed on LPAR.

**Performance Management template**:

| PM Parameters | Description |
|---|---|
| Enable gathering of PM from this system | The value of this parameter will be initially set to false and if the customer needs to send the Performance data to IBM, they should turn this on. Once this is turned on, SA starts collecting PM from each of the monitored partitions on a daily basis. |
| Default time of day to collect data files | This parameter will allow the customer to set a time for the data collection. Normally this is set to a time between 2 AM - 5 AM. |
| Enable generating Internal errors | This option can be used to generate internal errors when the PM data collection or PM transmission fails. Email Alerts can be configured to notify about the SA internal errors. |
| Information | Additional information about performance management. |

**SNMP Notification Template**

**SNMP Notification Template Properties:**

| Properties | Description |
|---|---|
| Target Network Manager Host | Specify the Target Network Manager host that will be receiving the SNMP Trap Notification. |
| Community | Specify the Community (default is public). |
| SNMP Port Number | Specify the SNMP port number on the Target Network Manager. |
| Send Trap for PMRs with Pending Status | Set to TRUE, if you want a SNMP Trap sent PMRs in the "pending" state. |
| Send Trap for PMRs with Held Status | Set to TRUE, if you want a SNMP Trap sent PMRs in the "held" state. |
| Send Trap for Internal Errors | Set to TRUE, if you want a SNMP Trap sent for Service Agent internal errors. |

## Monitored machines folder

When a Client Hardware Management Console is added to the network, the following templates are associated with that monitored machine.

### Node Info template

**Note:** Remember, if you add a Client Hardware Management Console to the SA Hardware Management Console Gateway, you must change that Hardware Management Console to Client mode. Use **Change Service Agent mode - (server/client)** from **Service Agent - Hardware Management Console** of **Service Applications.**

| Parameters / Fields | Description |
|---|---|
| **Node Info** | **Same as Network Node Info** |

**Environment template:**

| Parameters / Fields | Description |
|---|---|
| **Environment** | **Same as Gateway Environment.** |

**Linux Hardware Service template:**

| Standard Template | Description |
|---|---|
| **Hardware Service** | **Same as Gateway Hardware Service.** |

## Additional machine templates

Additional templates can be added to every machine (both gateway server and monitored) to provide various functions and options customizing Service Agent to the individual company needs. To access these templates select your Gateway server or a monitored machine and click **Add** and then click **Child.**

### CallController template

The CallController template, by default is installed on the gateway server for optimum performance of the Service Agent system. As a general rule this should not be changed. However, if necessary, for load balancing of the Network any machine can run the Call controller.

**CAUTION:** There should only be one Call Controller assigned within the Service Agent System. Do not operate with more than one template at a time. Results are undefined and could result in damaging the Service Agent databases.

### Email Alert

By adding an Email Alert template, Service Agent can send an e-mail message to contacts relating all or limited machine problem information. You can define as many e-mail contacts as you require, but an e-mail server must be active and accessible.

**Email Alert Template**

| Properties | Description |
|---|---|
| Email Address | The e-mail address of the contact you wish to alert. |
| Email Subject | The default subject line for messages. |
| Email Server | The hostname of the mail server to be used. |
| Email Wait Time In Minutes | This field determines how long to wait in order to gather any additional notifications that may be generated. When the time specified is reached, all notifications are combined into one e-mail notification and sent to the e-mail address. |
| | ***Set the following flags True/False accordingly.***<br>*Set Urgent flag for sending immediately do not wait for e-mail delay.* |
| Cautions Enabled | An *Error Event* occurred that is considered a caution or informational entry. A PMR is not generated for it. |
| Failed Enabled | A SA *Error Even*t transmission failed to open a PMR on the IBM SDR. |
| Held Enabled | A SA *Error Event* entry was created and set to a Held status. |
| Pending Enabled | A SA *Error Event* entry was created and set to a pending status. |
| Opened Enabled | A SA *Error Event* transmission OPENED a PMR on the IBM SDR. |
| Closed Enabled | A SA *Error Event* transmission CLOSED a PMR on the IBM SDR. |
| Internal Errors Enabled | An internal operating problem has occurred. (e.g. inability to read a required file, or run a command, or anything that goes wrong with the operation of Service Agent). |
| Duplicate Enabled | Notification if a duplicate PMR is attempted to be opened. |
| Licensing Enabled | A notification will be send 0, 30 or 60 days prior to the date when License Key gets expired. |
| PTF Updates Enabled | The machine has received notification that PTF Updates are available for download. |
| SA Updates Enabled | The machine has received notification that Service Agent Updates are available for download. |
| Heart Beat Enabled | The machine failed a heart beat. |
| Test Emails Enabled | This contact should receive any test e-mail's sent. |
| EED Enabled | Notification issued if failed to send with PMR information. |

**Available buttons for the Email template:**

| Button | Description |
|---|---|
| OK | The OK button located at the bottom of the detail pane is active once data has been typed or changed in a field. Click **OK** to save all data typed. |
| Cancel | Click **Cancel** to cancel the current operation. |

## Call Log folder

The Call Log template displays the results of connections and transmissions to the IBM SDR. By viewing this log during the dialing or initial phase of a connection, real time updates are logged. Once connection is made and requests have been transmitted, a summary count of the request types and whether they were transmitted successfully are logged.

The summary counts overlay the description entries made during the connection phase.

**Note:** The summary counts only relate to whether the transmission was successful or not. It does NOT indicate whether the specific request was accepted or failed due to some internal process checking or rejection. To determine the results of a specific request, if available, you must look at the specific entry for the request in question. A successful result on the transmission does not necessary indicate a positive reply for a specific request.

**CallLog Display Columns:**

| Column | Description |
|---|---|
| Start Time Stamp | Time Stamp of when the transmission started. |
| Description | This column displays real time connection updates as the connection is made. Once the connection has ended final Success/Fail results are logged here. |
| Try | This column displays how many times or retries it took to make the connection. |
| TTY Baud | If baud rate established, posted connect speed or <none> |
| Snd | This column is not used. |
| Rcy | This column is not used. |
| Status | Icon status of transmission, Green Flag = OK |
| Type | Type of call, LIC (padlock), PMR, VPD Icon symbols |
| End Time Stamp | Time Stamp of when the transmission ended |

Table may be sorted on any field by dragging that field to the left side of table columns.

## Administration folder

### Enroll template

The Enroll template provides the capability of enrolling one or more defined machines. Holding the shift key while selecting the second machine will mark multiple machines for enrollment.

Within this template a simple machine list is displayed, in the detail pane to the right, for selection and enrollment.

When the Enroll selection in the Navigation pane is highlighted the Add and Delete buttons at the bottom are disabled.

Available buttons for the Enroll template:

| Button | Description |
|---|---|
| Open | Click Open to display node information of the selected machine. See section on Node Info for details. |
| Enroll | Click **Enroll** to enroll the selected machine(s) with IBM. |

### Manage Cluster Ids template

This template allows the assignment or removal of Cluster Type, Serial, and Model information to selected machines.

Select machine or machines to append the Cluster information to, and then push **Append Cluster ID to the Machines** pushbutton. A cluster detail window will allow for the entry of cluster information, and whether you should override any detected cluster information.

**Enter the Cluster Details**

| | |
|---|---|
| Cluster Type | Enter 4 digit type assigned to cluster |
| Cluster Serial | Enter 7 digit serial number assigned to cluster |
| Cluster Model | Enter 3 digit model assigned (alpha in capitals) |
| Override detected Cluster Details | Check to override, only if SFP fails to detect the right cluster info. |
| OK | Saves entered cluster data |
| Cancel | Returns to previous menu, no action taken |

Selecting **Remove Cluster ID from Machines** pushbutton will issue a Yes / No validation prompt and if Yes is pressed the cluster information will be removed from the selected machines.

### Data Compression Cycles

The Data Compression Cycles template allows for the automatic saving and restoration of the SA Gateway database. The ESS database is maintained within the Java ESS daemon memory space and is saved and restored daily. Old or unused data will be purged automatically from memory during this cycle if compression is enabled. The compression should always be enabled to keep the daemon running as smoothly as possible. If daily compression does not occur, then the **sares** process will force an ESS daemon restart.

The detail pane shows the next scheduled compression date and time, enabled status of compression, and allows one to set the daily timer for scheduled compression or immediate execution. Using the **Compress Data Now** will immediately invoke a compression cycle, where the ESS process will shutdown, restart, and initialize the database. The Next Compression Date will be updated to reflect the new daily cycle time in 24 hours from the current time. A new cycle time may be set by entering the desired time either in a 12 or 24 hour format and then selecting the **Set The Timer For Data Compression** pushbutton. If entry is valid then the Next Compression Date will reflect the new time. If improper data entry is made a RED Time error will be posted and date will not be adjusted. Use the format display at the bottom of the window to assist you in the correct format for entering the time setting.

**Data Files template**

The Data Files template allows for the management of various collected data files for the configured Hardware Management Console machines. This template allows for the removal of old or unnecessary vital product data, extended error data files or PM data files that are maintained by SA for selected Hardware Management Console hosts.

Available buttons for the Data Files template:

| Button | Description |
|---|---|
| Open | Click Open to display node information of the selected machine. See section on Node Info for details. |
| Data Files Manager | This selection allows secondary window to select the type of file to be removed from the selected host database. The Data File Types are **eed, vpd, pm** which may be selected from a dropdown. The number of the selected file type will be shown, and the full filenames will be posted for selection. Selected files will be removed when the **Remove** pushbutton is activated. Pressing the Cancel will return to the previous menu without taking any actions. |

**Import / Export template**

The Import / Export template allows for the automatic addition of machines from an ASCII input file, the capability of saving existing machine entries to an ASCII output file, and exporting the defined database to an ASCII file and importing a previously exported database**.**

**Import ASCII Input File Format**:

Each monitored machine to be added must be on a single line. Each line must contain the required machine data in the following order with comma separators and no spaces.

**Note:** Processor ID is obtained by executing uname -m command on the physical host**.**

**“Hostname”**,**“Type”, “Serial”, “ProcessorID”, "Model", ”HMC”**

**For example, the input file would contain:**
ABC,7040,43515,003555434C00,681**,**HMC

sdr6k7.austin.ibm.com,7040,8386522,i686,681**,**HMC
**....**
XYZ,7040,34789,4438902**,,**HMC

"**HMC**" is a hard coded String, to identify this is an Hardware Management Console system. (not standalone SA which runs on the AIX partition)

**Available Buttons:**

| Button | Description |
|---|---|
| ASCII Input Machine List | Click **ASCII Input Machines List** to input an ASCII machine list. Type the location and name of the file at the selection window. |
| ASCII Output Machine List | Click **ASCII Output Machines List** to output an ASCII machine list of all defined Service Agent machines. Type the destination and name of the file at the selection window. |
| Export Service Agent Database | Click **Export Service Agent Database** to output the SA Gateway database to a file. |
| Import Service Agent Database | Click **Import Service Agent Database** to input a previously exported machine database file. |

**Lockout Machines template**

The Lockout Machines template allows turning off or locking out Service Agent on selected machines. This is useful when there is to be some type of system maintenance that could possibly cause Service Agent to report false errors. To avoid confusion lockout the system that you wish to ignore prior to performing any activities that could cause false errors.
**CAUTION:** The locked out system will not report any errors until the lock is removed. Be sure to unlock the system after all maintenance work is performed.

**Available Buttons:**

| Button | Description |
|---|---|
| Open | Click **Open** to see Node information details on the selected machine. |
| lock | Click **lock** to lock the machine and disable Service Agent reporting. |
| unlock | Click **unlock** to unlock the machine and enable Service Agent reporting. |

### Purge data template

The Purge data template allows you to purge all the data collected and placed in the CallLog folder, information associated with PMR and Error data contained in database, and queued data. The CallLog folder is located beneath the Network folder in the Navigation Pane. PMR and Error information are shown under machine detail. The outgoing queue cannot be viewed but contains any pending actions that are to go to the IBM SDR on next established good connection. Be aware if you purge the outgoing queue that pending information may be lost or not transmitted to IBM. The Email Lock is set once a Revision Update notification has been sent, this may be reset by setting that selection to true.

**Available Buttons:**

| Button | Description |
|---|---|
| | |
| Purge | Click **Purge** to optionally purge all the following data:<br><br>• CallLog Data - Clears the CallLog<br>• Error Warnings - Clears accumulated Error Warnings<br>• Internal Errors - Clears accumulated Internal Errors<br>• Closed PMR - Clears PMRs with a Closed status<br>• All PMR - Clears all PMRs from the database<br>• Outgoing Queue - Removes pending entries in the outgoing queue and sets the status to Fail<br>• Email Locks for Revision Updates - Removes any locks set |

### SA Access template

This template allows the assignment of a new password for Service Agent User Interface access. Pressing the Change the Password pushbutton will bring up a window prompt where old and new password information may be entered. The keystrokes will be shown with * filled for key stroke verification.

**Enter the Password Details**

| | |
|---|---|
| Old Password | Enter the current SA access password |
| New Password | Enter the new password data |
| Verify New Password | Enter the new password again for verification |
| OK | Verifies and saves entered data |
| Cancel | Returns to previous menu, no password action taken |

## Alerts folder template

**The Alerts template allows for screen display.**
Alerts are generated by SA when important events occur, such as status changes to PMRs or SA internal errors. In addition to the e-mail alert notification other alert methods can be displayed on the screen. As long as the selection is open, configured alerts are displayed and maintained in the detail pane window. When the selection is closed and reopened the screen is cleared for new alerts. By default all alerts are enabled for display in the Alert selection. Specific alerts can be ignored by setting the associated toggle buttons to true.

**Available entries for Alert template:**

| Alert | Description |
|---|---|
| Limit | Number of Alerts that are kept at one time. When the limit is reached, no more entries are displayed until the window is cleared or the limit is increased. |
| Alerts | This is the display capture window for Alerts |
| Open | To view details of an alert entry, select it from the Alerts window and click **Open**. |
| Reset | To clear the list entries from the alert window press this button. |
| Flag | The following alerts can be prevented from displaying by setting ignored flag. |
| Cautions ignored | To ignore “Cautions” alerts, set this toggle button to true. |
| Closed ignored | To ignore “Closed” alerts, set this toggle button to true. |
| Failed ignored | To ignore “Failed” alerts, set this toggle button to true. |
| Held ignored | To ignore “Held” alert, set this toggle button to true. |
| Internal Errors ignored | To ignore “Internal Error” alerts, set this toggle button to true. |
| Opened ignored | To ignore “Opened” alerts, set this toggle button to true. |
| Pending ignored | To ignore “Pending” alerts, set this toggle button to true. |

## Filter lists folder

### Resource Filters template

The Resource Filters template works in conjunction with the Add / Forms / Resource Filter template. When this template is selected all resources that have been configured to be ignored are displayed.

If this template is blank, then no resource filters have been added to the Service Agent Network tree.

For details on adding Resource Filters, see *How to define Resource Filters* in Chapter 5.

Once resource filters have been defined, clicking on this template changes the detail pane into two sections. The upper section has a list of all of the resource filters indicating the Source or machine the resource filter has been added to and the name of the resource that is being ignored.

The lower section displays the Node Information associated with the source or machine that the filter was added to. This display changes depending upon which source or machine is selected.

### Thresholds template

*The Thresholds template works in conjunction with the Add Form Threshold template.*

When this template is selected, all thresholds that have been configured are displayed. If this selection is made and the display is blank, no additional thresholds have been added to the Service Agent Network tree.

For details on adding Thresholds , see *How to specify Thresholds* in Chapter 5.

Once a threshold has been defined, clicking the Thresholds template makes the detail pane appear in two sections.

The upper section has a list of all of the thresholds with the specific configuration information set for each threshold. The bottom section displays the information details of the machine the threshold was added to or the information details of the Network if the threshold was added to the network. In addition there is an Overrides entry in this section which displays the name of the source or machine this threshold overrides.

For example, if threshold error 124-708 is added to the Network and the same threshold error number 124-708 is added to a specific machine with different configuration data, then the threshold added to the machine would take precedence or an override threshold configured for the Network when it occurs on that machine. If the error occurs on any other machine, then the threshold for the Network applies.

## Manual Tools folder

### Connect template

The Connect template provides the capability to connect to the IBM Service data receiver (SDR) immediately or force a current connection to be canceled. It can be used in situations where there are pending requests that should go out immediately or where there is a need to verify the external connection process is working properly.

When connection is made to the SDR, any pending requests destined to be sent to IBM are handled. If there are no pending requests, then a simple handshake between Service Agent and the SDR is performed and the connection is ended.

The Disconnect is use to break any current connection established with IBM, either the Internet or the dialer connection is broken at next logical break.

**Available Buttons for Connect template:**

| Buttons | Description |
|---|---|
| Connect | Click **Connect** to initiate an immediate connection to SDR. |
| Disconnect | Click **Disconnect** to disconnect the current connection to SDR. |

**Microcode template**

Microcode Download capability has been sunset and superseded by the Microcode Discovery Service available at : http://techsupport.services.ibm.com/server/aix.invscoutMDS

**PMR template**

The Manual PMR allows the creation of a PMR for the selected machine and sends it to the IBM SDR. Initial selection of controlling Hardware Management Console machine where PMR will be posted must be made and the Generate button will then be activated. This will bring up a selection window listing all of the machines supported on the selected Hardware Management Console for final selection of PMR information. Selecting the machine and pushing OK will post the final creation window with pre-filled information from selected host. Although any of the fields may be changed it is suggested that only Error Number, Description, and Error Details be updated.

Only Hardware PMRs may be created currently. The Software selection is for future requirements.

Pressing the Generate push button once fields are filled in will give you a choice to dial immediately or a delayed request to IBM SDR. While the Cancel push button will return to main Manual PMR window with no action taken.

**Collect VPD**

This option can be used to manually collect VPD from each of the client Hardware Management Consoles. SA on each of the Hardware Management Console client will try to pull VPD from the monitored systems and send it to the gateway. If it fails during this process, an internal error will be created and e-mail notifications may be send if an e-mail alert is set to notify the users.

After collecting the VPD, check the CEC folder under each of the Hardware Management Console to verify what has been collected.

***Send VPD***

The VPD template gathers the latest Vital Product Data (VPD) from the selected machine and sends it to the IBM SDR.

In those instances where the most current copy of VPD is needed by IBM support for problem analysis, this selection bypasses the VPD timer configuration. You have the option to wait for the next time Service Agent calls SDR, or you can make a connection and immediately send the VPD.

For information on configuring the VPD template, see *How to send VPD* data in Chapter 5.

***Save VPD data to file***

Saving VPD data to a local file is possible using the *Save VPD* option under the Manual Tools folder.

Select the machine for which the VPD data needs to be saved and click **Save VPD Data to File**.

A file save dialog box pops up. The VPD data can be saved in two formats.

1. Text Format - Choose the *Files of Type* as text files (*.txt) and choose the file name and click on **Save**.

2. ZIP Format - Choose the *Files of Type* as zip files (*.zip) and choose the file name and click on **Save**. The file will be in zip format with a .zip extension. Use *unzip -j* to unzip the file.

If the destination for the file is a diskette, the program may fail if the diskette is full and does not prompt for the next diskette to be inserted. Hence the save process stops in the middle.

**Performance Data**

Performance Data template gathers the latest PM data using the selected Hardware Management Console system from its monitored systems and sends it to the IBM SDR.

***Collect PM***

This option will collect the PM Data from the monitored systems, using the selected Hardware Management Console system. There might be multiple LPARs being monitored by a single Hardware Management Console. It is done in two phases. First, the data will be collected from the AIX partitions and then it will be moved to the gateway system, if the Hardware Management Console is a client to another gateway Hardware Management Console.

***Send PM***

This option will send the collected PM data to IBM manually.
Use both the Collect and Send options to manually re-send the PM data to IBM.

## Test Tools folder

### TestEmail

The Test Email template allows you to verify the proper operation of the Email Alert templates that have been added. This selection sends a test e-mail notification to all Email Alert templates that have the Test Email option turned on or set to TRUE. If an e-mail address should not get *Test Notifications* this option should be switched to FALSE.

See section on "Adding Email Alert" templates for details. If an e-mail address fails to receive a test notification, check to make sure the Email alert and the test Email check box are set to TRUE. If they are, then examine your local Email system configuration and set up to ensure it is working property. Service Agent sends Email notifications using the simple AIX *sendmail* command as a typical client. All other aspects of the local mail system are under control and responsibility of the user or local administrator

### TestPMR

The TestPMR template sends a test problem management report to the IBM SDR. Upon receiving this report contact is made back to the customer indicating proper reception of the test PMR. This is used to verify the machine can properly open a PMR into the IBM system. If contact with IBM support is not made within a reasonable time after the PMR has been successfully opened, contact IBM support or your normal channel of access to verify it's arrival. Be ready to supply the PMR#, machine type, and serial number of the machine it was opened against.

### Test SNMPTrap

The Test SNMPTrap template sends a test SNMP event to all Service Agent clients configured to listen for the event. These Service Agent clients then in turn generate an SNMP trap notification and send it to their designated SNMP Target Host.

# Appendix B. Accessing the SA interface using a PC

You can access the Service Agent interface using a PC with Microsoft Windows and Java environment.

Create the PC interface by completing the following steps:

__ 1. On the Hardware Management Console Gateway server, run the file /usr/svcagent/bin/installnt. Running *installnt* creates a tar file called *instui.tar* located in the /tmp directory.

__ 2. Transfer the *instui.tar* file to the PC from which you want to run the Service Agent interface.

__ 3. Unzip instui.tar.
The unziped file contains a working directory called *svcagentui*. Additionally, /var/svcagent and /usr/svcagent are built

__ 4. Locate the following files contained in svcagentui.

- hmcstartadvanced_java.bat - starts the Service Agent Advanced Configuration interface
- hmcstartadvanaced_jre.bat - starts the Service Agent Advanced Configuration interface

__ 5. Depending on your PC environment you will have to run one of the above files.

## Troubleshooting

**UI does not appear**
If the UI does not connect to the Gateway, check the properties.hsc file to see the gateway name is fully qualified and can be reached from the PC. You can edit the properties.hsc file located in the *svcagentui* directory to put the fully qualified hostname of the gateway.

# Appendix C. Service Agent Modem Setup

A TTY device must be available and configured on the gateway system. A modem is required. The modem is used to call the IBM Service data receiver (SDR). For security, only outbound calls are required by Service Agent so the auto answer capability of the modem should be disabled. An asynchronous modem with a minimum communications speed of 9600 baud and error correction (in the United States) is required. Please refer to local procedures in your country to see what the modem requirements are for Service Agent.

If you use any of these modems, complete the instructions below prior to using Service Agent.

### Configuring the 7852-400 Modem

The 7852 Model 400 is one of the modems of choice for Service Agent. From the factory, there are DIP switches on the side of the modem that need to be set to make asynchronous mode the default mode. Switch 12 needs to be set to the off (down) position for asynchronous mode. Switch 5 needs to be set to the off (down) position to disable auto-answer to meet the security requirement that modem will not answer. See the diagram below for proper settings of switches if necessary.

To setup and initialize the 7852-400 for operation:

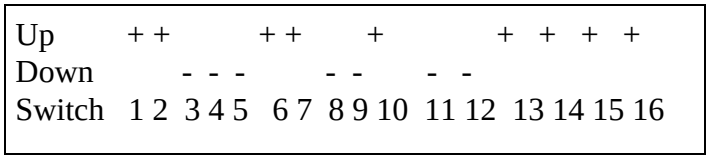
__ 1. Set switches 5 and 12 to the down (off) position.

__ 2. Connect the RS232 cable to the modem and to a serial port.

__ 3. Connect the telephone cable (sent with the modem) to the modem connector labeled LINE (middle connector), and to the telephone wall jack.

__ 4. Connect the modem power cable to the modem and the transformer to the building power.

__ 5. Power-on the modem (switch in rear).




*7852-400 Service Agent DIP Switch Settings*

**Configuring the 7857-017 or 7858-336 Modem**

The 7857 is another one of the modems of choice for Service Agent. The 7858-336 is the replacement modem for the 7857. These procedures are here to aid in the proper configuration of the 7857-017 or 7858-336, or to set a known configuration state.

To setup and initialize the 7857-017 or 7858-336 for operation:

__ 1. Connect the RS232 cable to the modem and to a serial port.

__ 2. Connect the telephone cable (sent with the modem) to the modem connector labeled PSTN, and to the telephone wall jack.

__ 3. Connect the modem power cable to building power.

__ 4. Power-on the modem.

__ 5. Wait for the main display panel.

Use the following procedure to place the modem in a known configuration.

After the modem is powered on and local tests have completed, there should be two lines of configuration information displayed on the modem LCD screen.

__ 1. Press the down arrow key 12 times until the CONFIGURATIONS message is displayed.
  ↓ CONFIGURATIONS D12
  Press →
__ 2. Press the right arrow key until the Select Factory message is displayed.
  → CONFIGURATIONS D12
  Select Factory_
__ 3. Press the Enter key to select the Factory configuration option.
Press the up arrow key until 0 is displayed.
  ↑ CONFIGURATIONS D12
  Select Factory 0
__ 4. Press the Enter key to load the predefined factory configuration 0.
  IBM 7857 AT CMD aa ■
  td_ rd_ dsr_ ec ■ ll_
__ 5. Press the down arrow key 7 times until the S-REGISTER message is displayed.
  ↓ S-REGISTER D7
  Press →
__ 6. Press the right arrow key until the message Ring to answ. on is displayed.
  → S-REGISTER D7
  Ring to answ. On=2_

__ 7. Press the Enter key to select Ring to answ. on.
S-REGISTER D7
Ring to answ. On=_
__ 8. Press the up arrow key until 0 is displayed.
↑ S-REGISTER D7
Ring to answ. On=0
__ 9. Press the Enter key to set Auto Answer to 0.
S-REGISTER D7
Press ➔
__ 10. Press the down arrow key 5 times until the CONFIGURATIONS message is displayed.
↓ CONFIGURATIONS D12
Press ➔
__ 11. Press the right arrow key 3 times until the Store User Conf. message is displayed.
➔ CONFIGURATIONS D12
Store User Conf._
__ 12. Press the Enter key to select the Store User Configuration option.
Press the up arrow key until 0 is displayed
↑ CONFIGURATIONS D12
Store User Conf. 0

__ 13. Press the Enter key to select location 0.

__ 14. Press the Enter key to save current configuration into User 0 .
CONFIGURATIONS D12
Press ➔
__ 15. Press the Enter key to return to main display panel.
IBM 7857 AT CMD aa_
td_ rd_ dsr_ ec ■ ll_ ■ = Shows LCD as on.

The above setup places the 7857 or 7858 modem into the proper configuration for use with the Dialer that is used for Service Agent pSeries or RS/6000.

**Notes:**
The modem initialization strings provided are on an AS IS basis. Although they have been tested in a typical AIX environment they may have to be modified depending on the actual setup and configuration of your environment.

# Appendix D. SNMP Notification Examples

## Hardware Problem

Enterprise ibmSaNotifications (1.3.6.1.4.1.2.6.205) community public
generic trap:6 specific trap:2
Timestamp:1060369 Agentaddr:psa3.raleigh.ibm.com args(7):
[1] private.enterprises.ibm.ibmProd.205.2.1.0 (OctetString): Service Agent Call Placement Test
[2] private.enterprises.ibm.ibmProd.205.2.2.0 (OctetString): psa3.raleigh.ibm.com
[3] private.enterprises.ibm.ibmProd.205.2.3.0 (Integer): 2
[4] private.enterprises.ibm.ibmProd.205.2.4.0 (OctetString): 7026-B80_104A11F
[5] private.enterprises.ibm.ibmProd.205.2.5.0 (OctetString): disk0
[6] private.enterprises.ibm.ibmProd.205.2.6.0 (OctetString): pSeries Service Agent. Ver R3.3.0.0
[7] private.enterprises.ibm.ibmProd.205.2.7.0 (OctetString): AIX

## Service Agent Internal Error

Enterprise ibmSaNotifications (1.3.6.1.4.1.2.6.205) community public
generic trap:6 specific trap:3
Timestamp:1082900 Agentaddr:psa3.raleigh.ibm.com args(4):
[1] private.enterprises.ibm.ibmProd.205.3.1.0 (OctetString): Enroll Failed - CONNECTIONPROBLEM - Enroll
[2] private.enterprises.ibm.ibmProd.205.3.2.0 (OctetString): psa3.raleigh.ibm.com
[3] private.enterprises.ibm.ibmProd.205.1.6.0 (OctetString): pSeries Service Agent. Ver R3.3.0.0
[4] private.enterprises.ibm.ibmProd.205.1.7.0 (OctetString): AIX

# Appendix E. Notices and Trademarks

## Notices

This information was developed for products and services offered in the U.S.A..

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in the area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject mater described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could contain technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of information which has been exchanged, should contact:

IBM Corporation
Department 80D
P.O.Box 12195
3030 Cornwallis
Research Triangle Park
NC 27709
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM international Program License Agreement or any equivalent agreement between us.

## Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

IBM
RS/6000
pSeries
Electronic Service Agent

Microsoft, Windows and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

Java is a trademark of Sun Microsystems

Other company, product, and service names may be trademarks or service marks of others.

# Hardware Management Console to SA Cross Reference

Red splash old Independent Catcher SAS end-of-service June 30, 2005.

| Hardware Management Console level | Description | SA level | Description |
|---|---|---|---|
| Hardware Management Console 1.1.0 | Hardware Management Console<br>Build level 20011128.1<br>RedHat 7.2 OS Ver 2.4.9-12<br>SA on base WSM menu | H1.0.0.1<br>Nov 30,2001 | SvcAgentHSC-1.0.0-1<br>Dialer phone pull down<br>SC38-7107 First Nov 2001 |
| Hardware Management Console 1.1.2 | Hardware Management Console<br>Build level 20020103.1<br>RedHat 7.2 OS Ver 2.4.9-12<br>SA on base WSM menu | H1.0.0.1<br>Nov 30,2001 | SvcAgentHSC-1.0.0-1<br>Dialer phone pull down<br>SC38-7107 First Nov 2001 |
| Hardware Management Console 3.1.2 | Hardware Management Console<br>Build level 20021110.1<br>RedHat 7.2 OS Ver 2.4.9-31 | H1.2.0.0<br>Oct 08,2002 | SvcAgentHSC-1.2.0-0<br>SA UI Registration/Customization<br>Dialer no default US country<br>SC38-7107 First Dec 2001 |
| Hardware Management Console 3.1.3 | Hardware Management Console<br>Build level 20030305.1<br>RedHat 7.2 OS Ver 2.4.9-31 | H1.2.0.2<br>Feb 12,2003 | SvcAgentHSC-1.2.0-2<br>SA UI Registration/Customization<br>Dialer default to US country<br>SC38-7107 First Dec 2001 |
| Hardware Management Console 3.2.0 | Hardware Management Console<br>Build level 20030410.1<br>RedHat 7.2 OS Ver 2.4.18-27.7.x | H2.0.0.0<br>Feb 12,2003 | SvcAgentHSC-2.0.0-0<br>SA UI Registration/Customization<br>SA Doc second edition Sep 2002 |
| Hardware Management Console 3.2.1 | Hardware Management Console problems, not in field | H2.0.0.0 | SvcAgentHSC-2.0.0-0 |
| Hardware Management Console 3.2.2 | Hardware Management Console<br>Build level 20030528.1<br>RedHat 7.2 OS Ver 2.4.18-27.7.x | H2.0.0.0<br>Feb 12,2003 | SvcAgentHSC-2.0.0-0<br>SA Doc third edition Jan 2003 |
| Hardware Management Console 3.2.3 | Hardware Management Console<br>Build level 20030818.1<br>RedHat 7.2 | H2.0.0.2<br>Jun 26,2003 | SvcAgentHSC-2.0.0-2<br>SA UI Registration/Customization<br>SA Doc third edition Jan 2003 |

## Blue Splash goes to Service Data Receiver (SDR) uses SACM.

| Hardware Management Console level | Description | SA level | Description |
|---|---|---|---|
| Hardware Management Console 3.2.4 | Hardware Management Console Build level 20030919.1 | H3.1.0.0 Sep 16,2003 | SvcAgentHSC-3.1.0-0<br>www-3 207.25.251.251<br>No /etc/resolv.conf selection<br>SA Doc fourth edition Sep 2003 |
| Hardware Management Console 3.2.5 | Hardware Management Console problems , not in field | H3.1.0.1 | SvcAgentHSC-3.1.0-1 |
| Hardware Management Console 3.2.6 | Hardware Management Console Build level 20040113.1<br>Last Red Hat 2.78 | H3.1.0.2 Dec 5,2003 | SvcAgentHSC-3.1.0-2<br>www-306 207.25. 251.249<br>Use /etc/resolv.conf selection |
| Hardware Management Console 3.3.0 | Hardware Management Console Build level 20040505.1<br>MPC | H3.1.0.3 Feb 18,2004 | SvcAgentHSC-3.1.0-3<br>www-306 207.25.251.249<br>Use /etc/resolv.conf selection |
| Hardware Management Console 3.3.1 | Hardware Management Console Build level 20040716:1<br>MPC | H3.1.0.3 Feb 18,2004 | SvcAgentHSC-3.1.0-3<br>www-306 207.25.251.249 |
| Hardware Management Console 3.3.2 | Hardware Management Console Build level 20040822:1<br>MPC | H3.1.0.3 Feb 18,2004 | SvcAgentHSC-3.1.0-3<br>www-306 207.25.251.249 |
| Hardware Management Console 3.3.3 | Hardware Management Console Build level 20041210:1<br>MPC | H3.1.0.7 Nov 16, 2004 | SvcAgentHSC-3.1.0-7<br>www-306 207.25.251.249 |
| Hardware Management Console 3.3.4 | Hardware Management Console Build level 20050218:1<br>MPC | H3.1.0.7 Nov 16, 2004 | SvcAgentHSC-3.1.0-7<br>www-306 207.25.251.249 |
| Hardware Management Console 3.3.5 | Hardware Management Console Build level 20050415:1<br>MPC | H3.1.0.8 Nov 29, 2004 | SvcAgentHSC-3.1.0-8<br>www-306 207.25.251.249 |
| Hardware Management Console 3.3.6 | Hardware Management Console Build level 20050706.1<br>MPC | H3.1.0.8 Nov 29, 2004 | SvcAgentHSC-3.1.0-8<br>www-306 207.25.251.249 |
| Hardware Management Console 3.3.7 | Hardware Management Console Build level 20060406.1<br>MPC | H3.1.0.8 Nov 29, 2004 | SvcAgentHSC-3.1.0-8<br>www-306 207.25.251.249 |
| Hardware Management Console 3.3.+ | Hardware Management Console Build level 20060630:1<br>MPC | H3.2.0.0 Nov 29, 2004 | SvcAgentHSC-3.2.0-0<br>207.25.252.200<br>129.42.160.48 |